Uji Penetrasi dengan BlankOn

Putu Wiramaswara Widya <initrunlevel0@gmail.com>
Mahasiswa Institut Teknologi Sepuluh Nopember, Surabaya

Perkenalkan diri saya...

Nama saya Wira

Lengkapnya **Putu Wiramaswara Widya**

Asli Bali Kuliah di Surabaya Di kampus ITS

Jurusan **Teknik Informatika (TC)**

Semester III

Pengalaman

- Di BlankOn
  - Menulis buku Panduan BlankOn 5.0 (Nanggar) (2009)
  - Berkontribusi pada fitur Aksara Nusantara (2010, 2012)
- Keilmiahan
  - Juara I Lomba Karya Tulis tingkat Provinsi 2009
  - Medali Emas Olimpiade Penelitian Siswa Indonesia (OPSI) 2010
  - Finalis Pekan Ilmiah Mahasiswa XXV Yogyakarta bidang PKM-KC
- Sekuritas Jaringan
  - Baru belajar :D
  - Juara III Lomba Sekuritas Jaringan GEMASTIK V

BlankOn

Materi Lokakarya Ini

- Penganalan **uji Penetrasi**
- Pengenalan **CEH**
- Langkah-langkah **Uji Penetrasi**
- Pemasangan **tool** pada BlankOn
- Cara **menggunakan** tool
- **Demo**

BlankOn

Asumsi Saya

Peserta lokakarya adalah orang **yang baru mengenal** uji penetrasi, CEH dan dunia heker-hekeran*

BlankOn

*) Saya heker nubi, ampun kk!

Uji Penetrasi dan CEH

BlankOn

Menurut Wikipedia...

A **penetration test**, occasionally **pentest**, is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process involves an active analysis of the

BlankOn

Uji penetrasi melakukan **apa yang dilakukan oleh peretas**, tetapi dengan **tujuan yang baik** untuk menghindari serangan dari peretas yang jahat di kemudian hari.

Siapakah orang yang melakukan hal ini?

BlankOn

Dapat
Sertifikasi

BlankOn

Jadi ada tiga jenis peretas di dunia ini :

- *Black Hat* :100% tujuan jahat, tanpa izin, gak sopan
- *White Hat* :100% tujuan baik, sopan, CEH
- *Grey Hat* : 50% baik 50% jahat

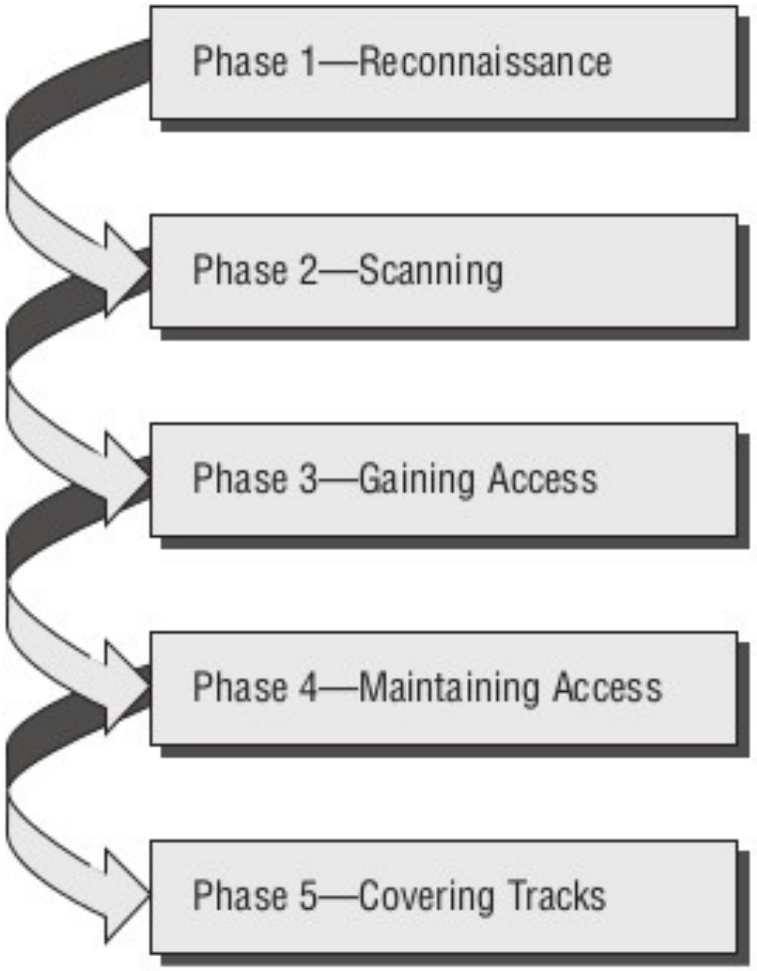
BlankOn

Metodologi *Hacking*

BlankOn

Langkah-langkah Uji Penetrasi

FIGURE 1.1 Phases of hacking



BlankOn

Persiapkan alat *heker* di BlankOn Linux

Tidak harus menggunakan **Backtrack**, Anda bisa melakukan uji penetrasi atau *heking* di BlankOn Linux anda dengan memanfaatkan lumbung paket dari Backtrack.

Persiapkan :

- OS BlankOn Linux versi apa saja (minimal 7.0 lah)
- Koneksi Internet untuk mengunduh paket

BlankOn

Persiapkan lumbung paket

Buka terminal, ketik perintah “sudo nano /etc/apt/sources.list”. Lalu tambahkan baris berikut :

deb http://192.168.0.28/backtrack/all revolution main microverse non-free testing

deb http://192.168.0.28/backtrack/32 revolution main microverse non-free testing

Simpan (Ctrl+X, W, Enter), lalu ketik perintah :
“sudo apt-get update”

BlankOn

Persiapkan lumbung paket

Beberapa paket juga sudah ada di lumbung paket BlankOn
Jadi pastikan pengaturan lumbung paket BlankOn sudah benar.

Ada juga beberapa perangkat lunak yang harus dipasang dari situs resmi pengembangnya.

Perhatikan! Kebanyakan alat yang digunakan mewajibkan hak akses *administrator* atau *root*.
Gunakan mantra sakti “sudo <nama-perintah>” untuk menjalankan suatu perintah dengan hak akses *root*.

BlankOn

Phase 1: Reconnaisance

BlankOn

Reconnaisance

Bagian dari skema **Footprinting**

Pada dasarnya tidak perlu menggunakan alat yang sangat canggih (Sudah tersedia pada umumnya sistem operasi). Hanya memerlukan kemampuan untuk “mengintai” yang baik.

BlankOn

Reconnaisance

Berbagai teknik *reconnaisanc*e menurut buku “CEH Exam Guide” :

- Domain Lookup
- WhoIs
- Traceroute
- Google
- **Social Engineering <-- top dan paling berbahaya**

BlankOn

Domain Lookup

```
root@wira-blankon:/home/wira# nslookup blankonlinux.or.id
Server:         202.46.129.2
Address:        202.46.129.2#53

Non-authoritative answer:
Name:   blankonlinux.or.id
Address: 72.20.8.13

root@wira-blankon:/home/wira#
```

BlankOn

Whois

www.whois.com/whois/facebook.com

Expiration Date: 30-Mar-2020

facebook.com Registrar Whois Updated 8 hours ago

MarkMonitor is the Global Leader in Online Brand Protection.

Domain Management
MarkMonitor Brand Protection™
MarkMonitor AntiPiracy™
MarkMonitor AntiFraud™
Professional and Managed Services

Visit MarkMonitor at www.markmonitor.com
Contact us at 1 (800) 745-9229
In Europe, at +44 (0) 203 206 2220

The Data in MarkMonitor.com's WHOIS database is provided by MarkMonitor.com for information purposes, and to assist persons in obtaining information about or related to a domain name registration record. MarkMonitor.com does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this Data only for lawful purposes and that, under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam); or (2) enable high volume, automated, electronic processes that apply to MarkMonitor.com (or its systems). MarkMonitor.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

Registrant:
Domain Administrator
Facebook, Inc.
1601 Willow Road
Menlo Park CA 94025
US
domain@fb.com +1.6505434800 Fax: +1.6505434800

Social Engineering

Paling berbahaya diantara segalanya.

Disebabkan oleh sifat murni “Manusia”.

Ada dua macem *Social Engineering :*

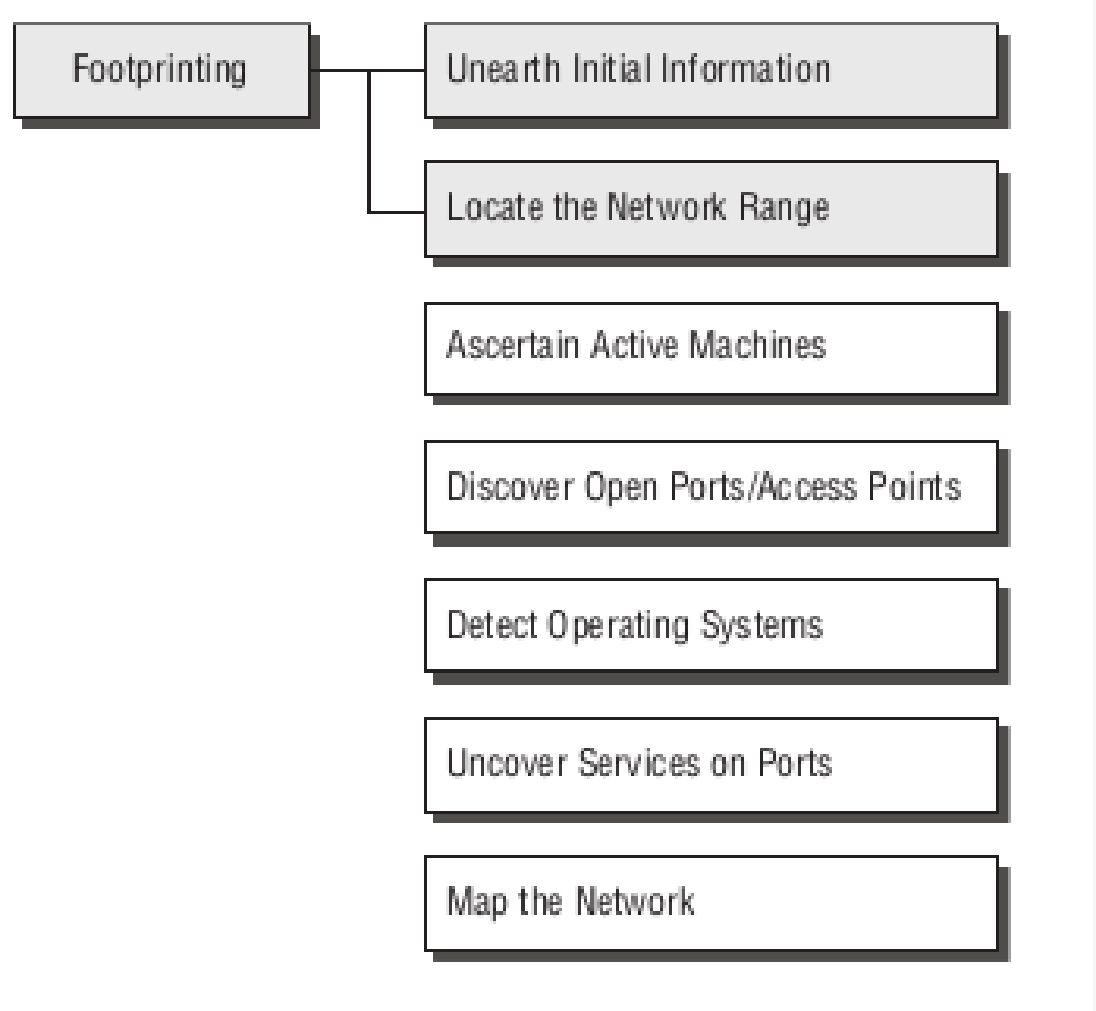
- Berbasis Manusia
- Berbasis Komputer

BlankOn

Phase 2: Scanning and Enumeration

BlankOn

Scanning and Enumeration



BlankOn

Nmap: pemindai *port*

Instalasi : “sudo apt-get install nmap”

Nmap merupakan alat untuk melakukan **pemindaian terhadap *port* yang terbuka** pada suatu komputer di jaringan.

Informasi yang didapatkan :

- Port yang terbuka
- Layanan yang disediakan komputer
- Sistem operasi dan versinya

BlankOn

Nmap: pemindai *port*

Mari cek komputer yang ada di jaringan ini.

Beberapa perintah umum

- nmap xxx.xxx.xxx.xxx/yy (Pemindaian satu jaringan dalam identitas jaringan)
- nmap xxx.xxx.xxx.xxx (Pemindaian satu *host*)
- nmap -sP xxx.xxx.xxx.xxx/yy (Pemindaian melalui Ping saja)
- nmap -O xxx.xxx.xxx.xxx (Pemindaian sistem operasi)

BlankOn

Nmap: pemindai *port*

```
Nmap scan report for 10.151.35.81
Host is up (0.00059s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1033/tcp open  netinfo
1035/tcp open  multidropper
1521/tcp open  oracle
5357/tcp open  wsdapi
MAC Address: 00:26:6C:B9:8B:3A (Inventec)
```

BlankOn

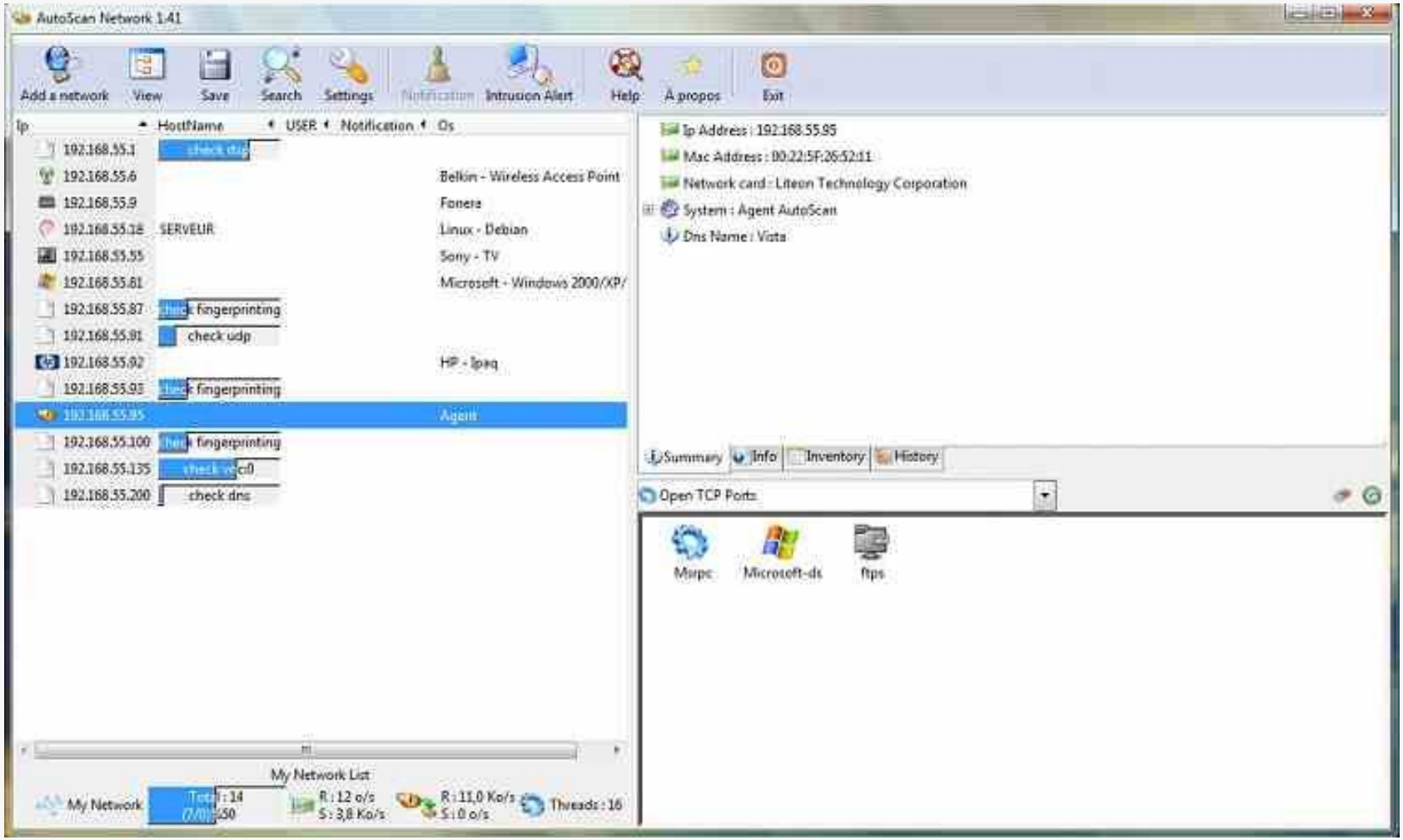
Alat pemindai yang lebih manusiawi

Bisa dipasang dari lumbung paket :

- Autoscan (sudo apt-get install autoscan) (Backtrack)
- Zenmap (sudo apt-get install zenmap) (BlankOn)

BlankOn

Autoscan



BlankOn

Mantra: Pemindai Aplikasi Web

Pada dasarnya merupakan peramban Firefox yang dimodifikasi untuk fitur uji penetrasi.

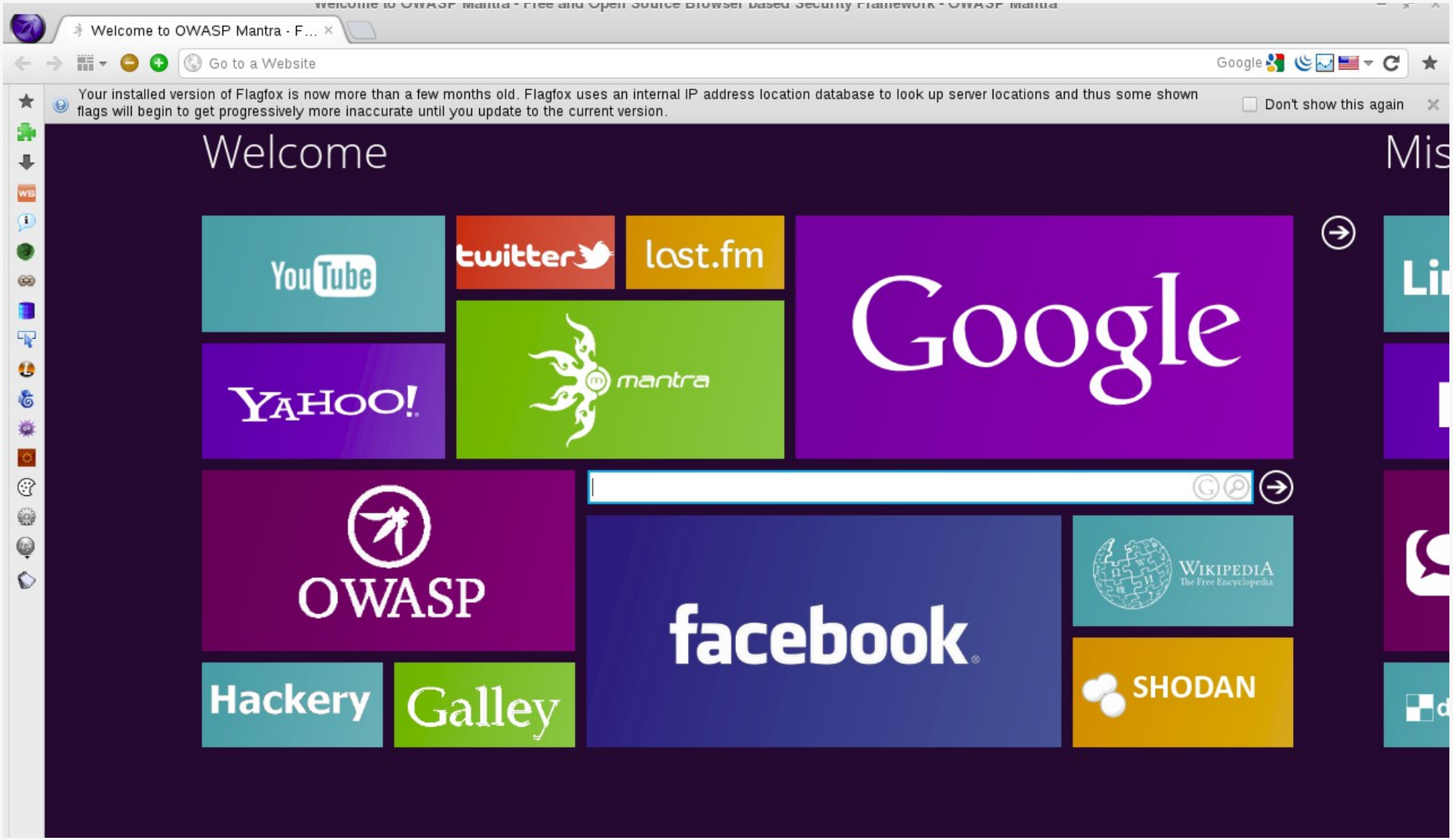
Instalasi : “sudo apt-get install mantra”

(Lewat lumket Backtrack)

Jalankan : “sudo /pentest/web/mantra/mantra”

BlankOn

Mantra: Pemindai Aplikasi Web



BlankOn

Kismet: Radar detektor WIFI

Kismet bisa digunakan sebagai radar untuk mendeteksi WIFI baik yang nampak atau yang disembunyikan sekalipun.

+ Kismet juga bisa melakukan *sniffing* paket nirkabel yang ada di sekitar (tapi kartu jaringan harus mendukung mode monitor)

BlankOn

Kismet: Radar detektor WIFI

Instalasi: sudo apt-get install kismet (Repo Backtrack)

Konfigurasi:

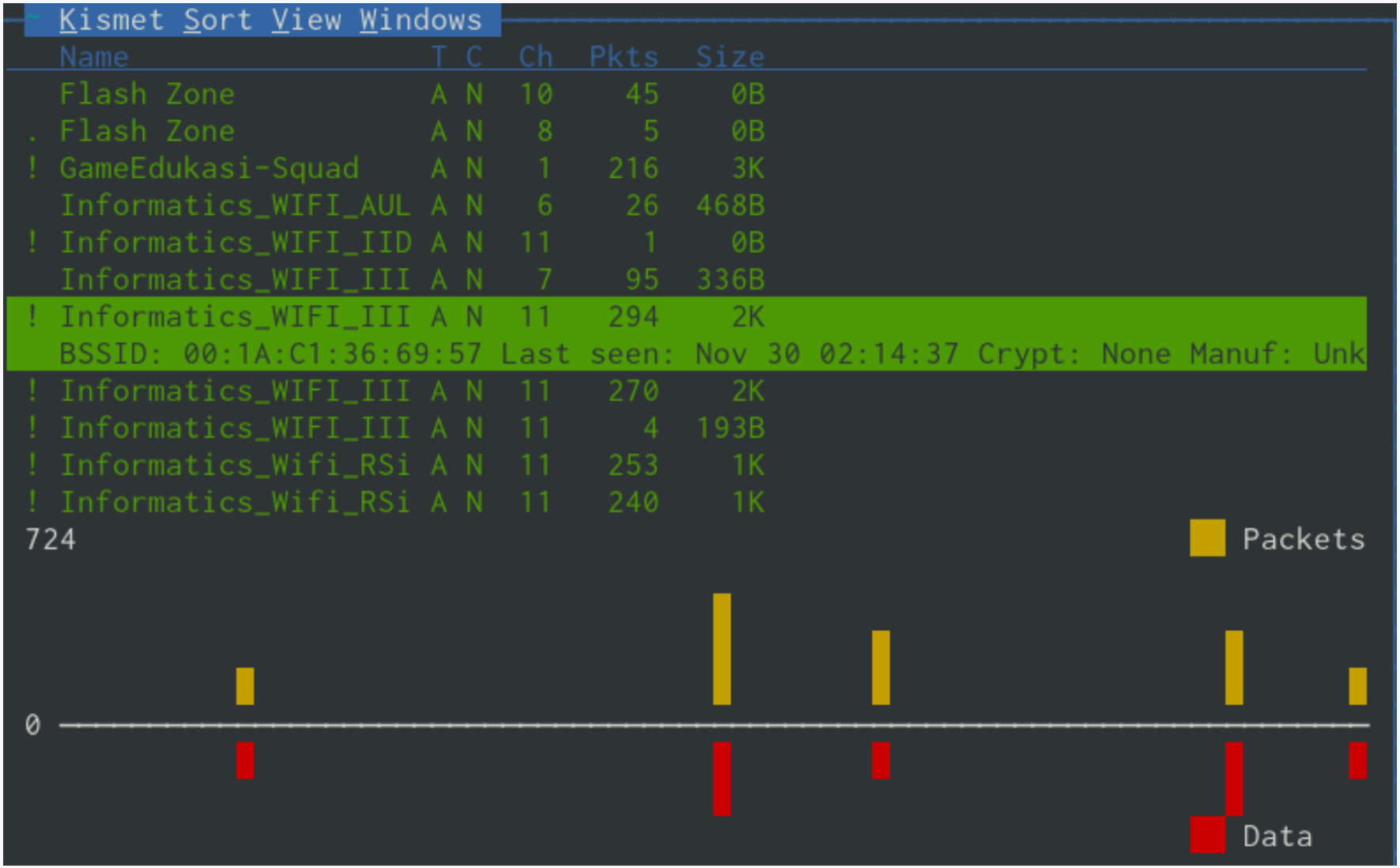
- Buka /usr/local/etc/kismet.conf
- Tambahkan baris :
  - ncsource=<interface-wlan>

    Misal :

    ncsource=wlan0
- Jalankan “kismet” sebagai root

BlankOn

Kismet: Radar detektor WIFI



BlankOn

Phase 3: Gaining Access

BlankOn

Berbagai langkah *heker*
Untuk mendapatkan akses

- Eksploitasi celah keamanan (*vulnerable attack*)
- Menanamkan *backdoor* atau *trojan*
- Social Engineering!

BlankOn

Eksploitasi Celah Keamanan

Pasti kita sering mendengar berita bahwa “ada celah keamanan baru pada perangkat lunak X dengan memanfaatkan kelemahan pada fitur Y”

Celah keamanan ini biasanya bagian dari cacat dari suatu perangkat lunak, jadi jika memang celah tersebut ditemukan dan belum ditambal, maka sang peretas akan memanfaatkan cacat tersebut untuk mengambil akses ilegal ke suatu layanan.

Celah keamanan juga bisa berasal dari kesalahan pengguna sendiri (Pengaturan bawaan yang dibiarkan)

BlankOn

Eksploitasi Celah Keamanan

Beberapa alat bantu menganalisa celah keamanan
- Nessus
- OpenVAS
- Dirbuster
- W3af
- Berbagai macam *script analyzer* siap pakai

Beberapa alat bantu untuk mengeksploitasi celah keamanan yang sudah diketahui :
- **Metasploit**
- **Mantra**
- Berbagai macam *script* siap pakai

BlankOn

Analisa Celah Keamanan

- Pada dasarnya membutuhkan kemampuan pemograman dengan menganalisa kode sumber perangkat lunak. http://www.phreedom.org/solar/exploits/exploit-code-development
- Juga harus memiliki kemampuan *reverse engineer* untuk perangkat lunak yang tidak ada kode sumbernya.
- Berbagai jenis celah keamanan yang diketahui bisa dilihat di situs-situs CVE (Salah satunya di http://web.nvd.nist.gov/view/vuln/search)
- Untuk pentester awammenguji, bisa menggunakan alat bantu analisa celah keamanan seperti : Nessus, OpenVAS, dll)

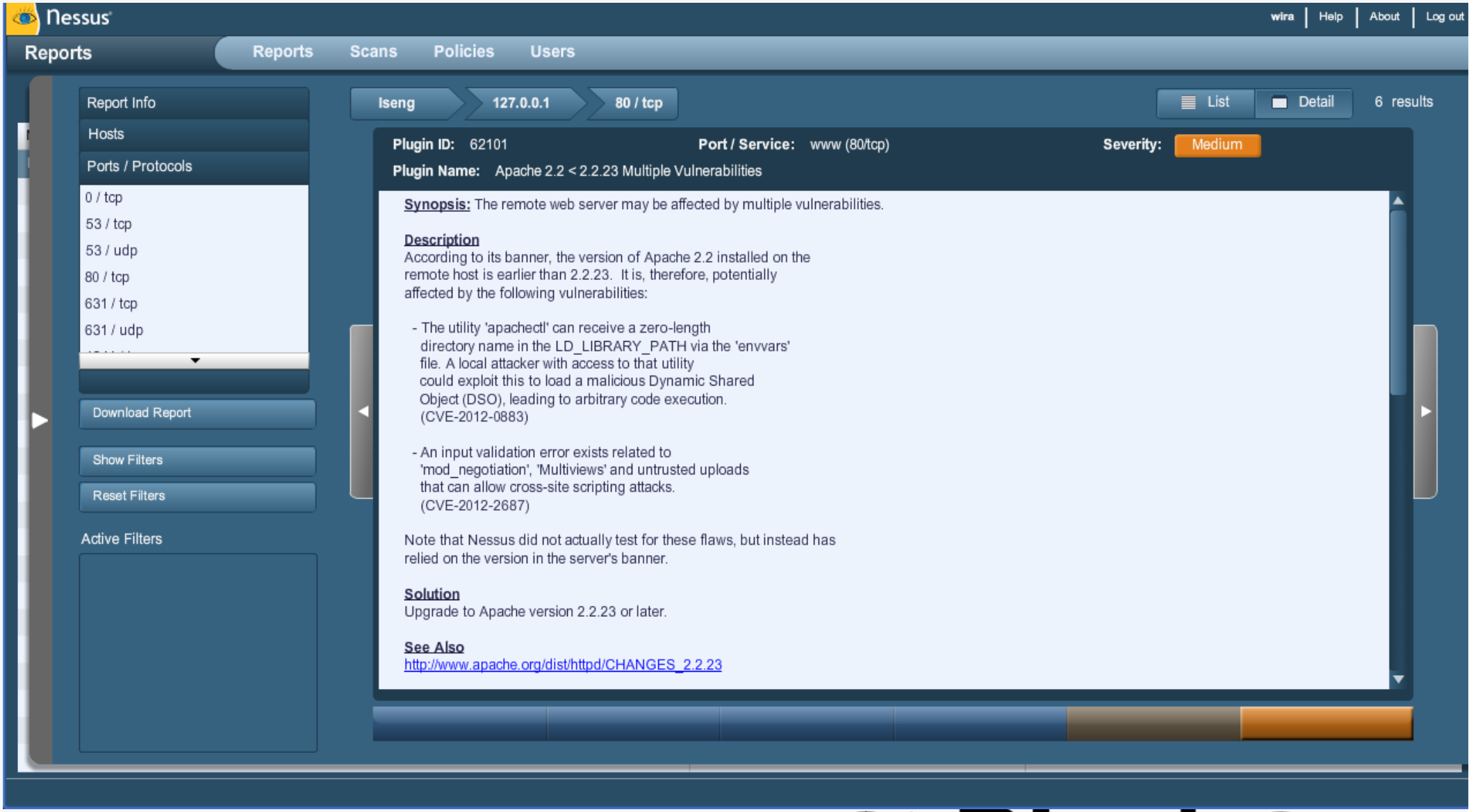
BlankOn

Nessus

- “sudo apt-get install nessus”
- Daftarkan terlebih dahulu melalui http://www.nessus.org/register/
- Jalankan “nessus-fetch –challenge” untuk mendapatkan plugin yang diperlukan. Masukan kode yang diberikan + kode aktivasi dari langkah sebelumnya ke https://plugins.nessus.org/offline.php.
- Unduh dan pasang plugin
  “sudo nessus-update-plugins ~/Downloads/all-2.0.tar.gz”
- Jalankan layanan Nessus
  “sudo service nessusd start”
- Buka https://127.0.0.1:8834.
- Untuk membuat pengguna baru, ketik perintah
  “sudo nessus-adduser”

BlankOn

Nessus



BlankOn

Metasploit: Vulnerability Exploit

“sudo apt-get install framework”
Atau bisa diunduh melalui situs http://www.metasploit.com/.

Fitur :

- Menyediakan beberapa jenis eksploit untuk berbagai macam sistem operasi dan aplikasi.
- Menyediakan alat bantu untuk membuat *backdoor*.
- Menyediakan alat bantu untuk beberapa jenis uji penetrasi kecil.
- Dapat ditambah dengan eksploit yang dibuat sendiri

BlankOn

Metasploit: Vulnerability Exploit

```
       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 488 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 488 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf >
```

BlankOn

Metasploit: Vulnerability Exploit

Kebanyakan berisikan exploit yang sudah banyak diketahui, dan kebanyakan sudah ditambal oleh vendor perangkat lunaknya (jika memang sudah rajin ditambal).

Tapi eksploit yang paling sakti adalah :
Backdoor + Social Engineering

http://www.offensive-security.com/metasploit-unleashed/Backdoorin
http://pentestlab.wordpress.com/2012/04/06/post-exploitation-disab

BlankOn

Metasploit: Vulnerability Exploit

Kebanyakan berisikan exploit yang sudah banyak diketahui, dan kebanyakan sudah ditambal oleh vendor perangkat lunaknya (jika memang sudah rajin ditambal).

Tapi eksploit yang paling sakti adalah :
Backdoor + Social Engineering

http://www.offensive-security.com/metasploit-unleashed/Backdoorin
http://pentestlab.wordpress.com/2012/04/06/post-exploitation-disab

BlankOn

W3af: Web Penetration Testing

Unduh dan baca dokumentasi cara pemasangan di http://sourceforge.net/projects/w3af/files/w3af/.

BlankOn

Apa saja masalah keamanan di Web?

- SQL Injection
  Menggunakan kelemahan aplikasi dalam mengolah input untuk menyuntikkan skrip SQL sakti
- XSS Injection
  Menggunakan kelemahan aplikasi dalam mengolah input untuk menyuntikkan skrip JavaScript berbahaya
- Session Hijacking
  Mencuri Cookie orang untuk dipakai sendiri

BlankOn

Yang lainnya, pelajari sendiri :D

Karena ilmu uji penetrasi sangat luas dan tidak cukup dibahas 2 jam, bagaimana kalau kita praktek langsung melakukan uji penetrasi.

- Siapkan laptop Anda
- Pasangkan ke WLAN dengan SSID “<apa-ya>”
- Silahkan cari mesin *server* yang akan ditarget.
- Selamat bereksplorasi

*) Sejujurnya, salindianya sudah banyak, jadi bosen aja sih :D

BlankOn

Referensi yang menarik untuk dibaca

- CEH: Study Guide (ISBN 978-0-470-52520-3)
- Hacking for Dummies (ISBN 978-0-470-55093-9)
- Bactrack 4: Assuring Security by Penetration Testing (ISBN 978-1-849513-94-4)
- http://www.offensive-security.com/metasploit-unleashed/Ma

BlankOn