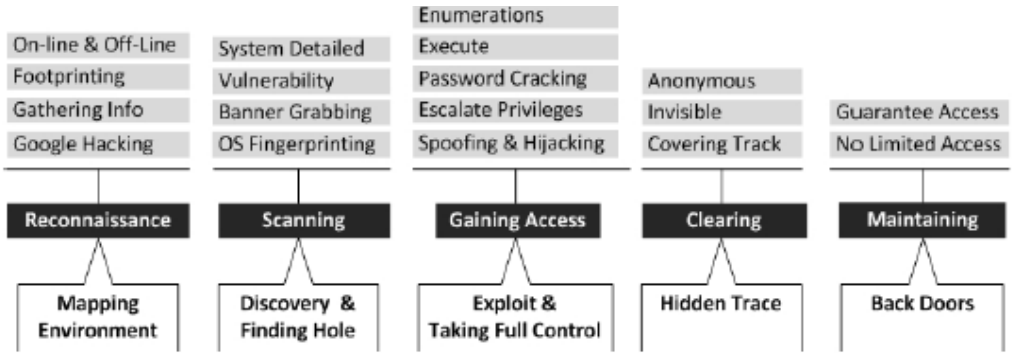
Dimas Wahyudi – 09011281320004 | Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com

Scanning

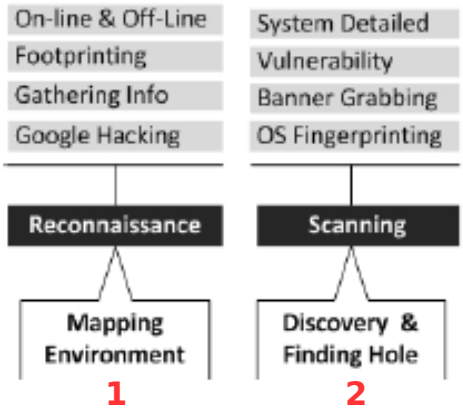
Dasar Teori : *Scanning*

Menurut *Certified Ethical Hacker* (CEH), Ada beberapa langkah dan teknik yang umumnya digunakan untuk mencoba menembus atau menyerang (*attack*) sebuah sistem, seperti terlihat pada gambar 1.



Gambar 1. Langkah dan teknik penyerangan (*attack*)

Sebelum melalukan tahapan *scanning*, tahapan *reconnaisaance* merupakan tahapan awal yang perlu dilakukan untuk memperoleh informasi dasar dari target yang akan dilakukan penyerangan (*attack*). Informasi yang diperoleh dari tahapan *reconnaisaance* diperlukan untuk melakukan tahapan *scanning*, seperti terlihat pada gambar 2.



Gambar 2. Tahap *(1) reconnaisaance* dan *(2) scanning*

Scanning merupakan tahapan awal dimulainya penyerangan (*pre-attack*). Dari *scanning* pernyerang (*attack*) akan mencari kemungkinan-kemungkinan yang dapat digunakan untuk mengambil alih sistem target, dan informasi yang didapatkan akan digunakan sebagai jalan masuk. Menurut *Certified Ethical Hacker* (CEH) tujuan dari tahapan ini adalah untuk memperoleh informasi berupa : *host* yang aktif, *IP Address*, *port* yang terbuka, *Operating*

System (OS), *System architecture*, *services* yang berjalan pada *host* dan *vulnerabilities.* Seperti pada gambar 3 berikut :

Gambar 3. *Objectives of Network Scanning*

Tahap 1 : *host* yang aktif, *IP Address*, *port* yang terbuka

```
C:\Users\Dr.Dimas Wahyudi>ping www.unsyiah.ac.id

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Reply from 202.4.186.223: bytes=32 time=123ms TTL=58
Reply from 202.4.186.223: bytes=32 time=70ms TTL=58
Reply from 202.4.186.223: bytes=32 time=70ms TTL=58
Reply from 202.4.186.223: bytes=32 time=77ms TTL=58

Ping statistics for 202.4.186.223:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 123ms, Average = 85ms

C:\Users\Dr.Dimas Wahyudi>
```

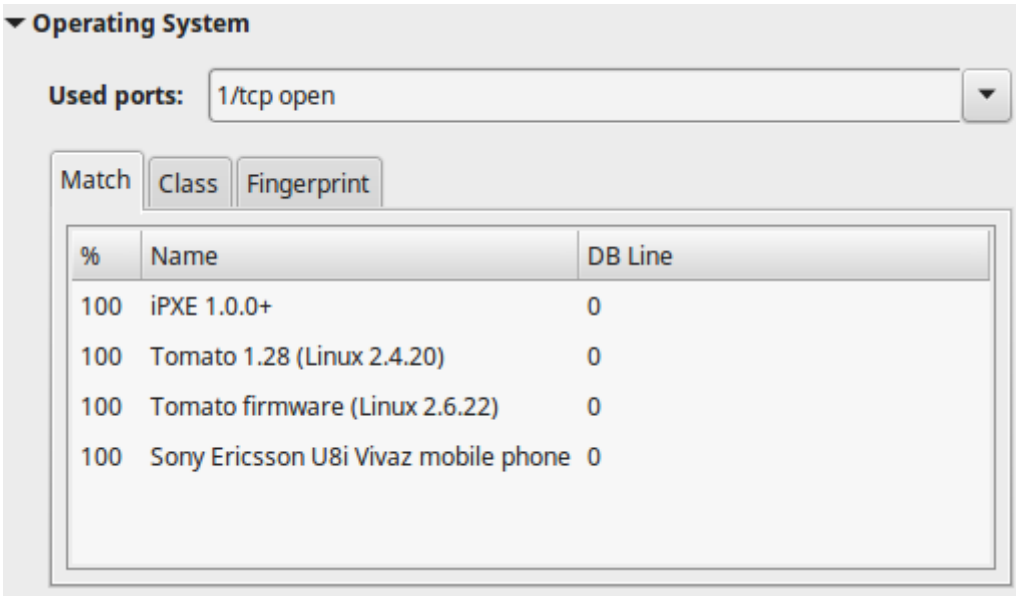
```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-02-22 13:35 WIB
Nmap scan report for unsyiah.ac.id (202.4.186.223)
Host is up (0.041s latency).
PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
26/tcp    open  rsftp
30/tcp    open  unknown
32/tcp    open  unknown
33/tcp    open  dsp
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
70/tcp    open  gopher
79/tcp    open  finger
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
```

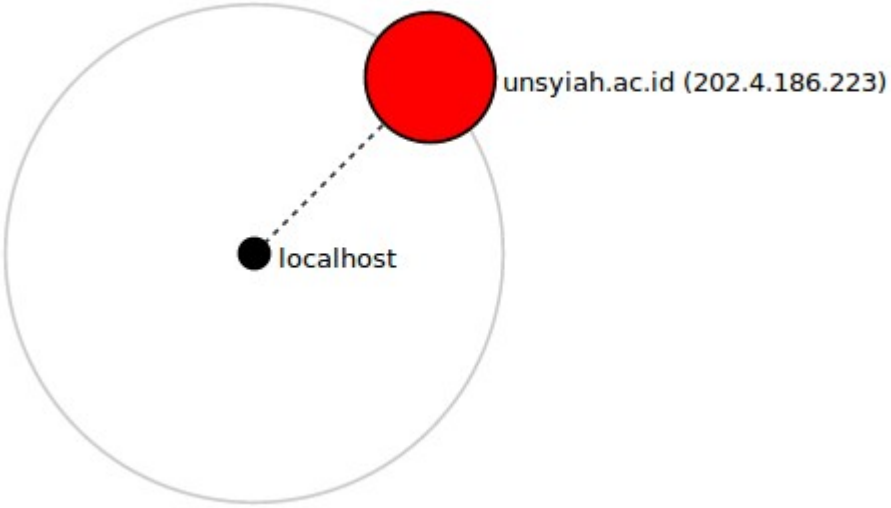
```
55600/tcp open  unknown
56737/tcp open  unknown
56738/tcp open  unknown
57294/tcp open  unknown
57797/tcp open  unknown
58080/tcp open  unknown
60020/tcp open  unknown
60443/tcp open  unknown
61532/tcp open  unknown
61900/tcp open  unknown
62078/tcp open  iphone-sync
63331/tcp open  unknown
64623/tcp open  unknown
64680/tcp open  unknown
65000/tcp open  unknown
65129/tcp open  unknown
65389/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.22 seconds
```

```
nmap -sn 202.4.186.223/24
Nmap scan report for 202.4.186.226
Host is up (0.033s latency).
Nmap scan report for 202.4.186.227
Host is up (0.035s latency).
Nmap scan report for 202.4.186.228
Host is up (0.033s latency).
Nmap scan report for 202.4.186.230
Host is up (0.048s latency).
Nmap scan report for 202.4.186.231
Host is up (0.047s latency).
Nmap scan report for 202.4.186.232
Host is up (0.033s latency).
Nmap scan report for 202.4.186.233
Host is up (0.035s latency).
Nmap scan report for 202.4.186.235
Host is up (0.033s latency).
Nmap scan report for 202.4.186.239
Host is up (0.034s latency).
Nmap scan report for 202.4.186.240
Host is up (0.035s latency).
Nmap scan report for 202.4.186.242
Host is up (0.042s latency).
Nmap scan report for 202.4.186.243
Host is up (0.035s latency).
Nmap scan report for 202.4.186.247
Host is up (0.035s latency).
Nmap scan report for 202.4.186.248
Host is up (0.035s latency).
Nmap scan report for 202.4.186.249
Host is up (0.035s latency).
Nmap scan report for 202.4.186.250
Host is up (0.035s latency).
Nmap scan report for 202.4.186.251
Host is up (0.033s latency).
Nmap scan report for 202.4.186.254
Host is up (0.033s latency).
Nmap done: 256 IP addresses (170 hosts up) scanned in 224.11 seconds
```

```
Service scan Timing: About 97.90% done; ETC: 12:50 (0:01:35 remaining)
Completed Service scan at 12:50, 4491.54s elapsed (1000 services on 1 host)
Initiating OS detection (try #1) against unsyiah.ac.id (202.4.186.223)
Retrying OS detection (try #2) against unsyiah.ac.id (202.4.186.223)
```

Tahap 2 : *Operating System* (OS) and *System architecture*

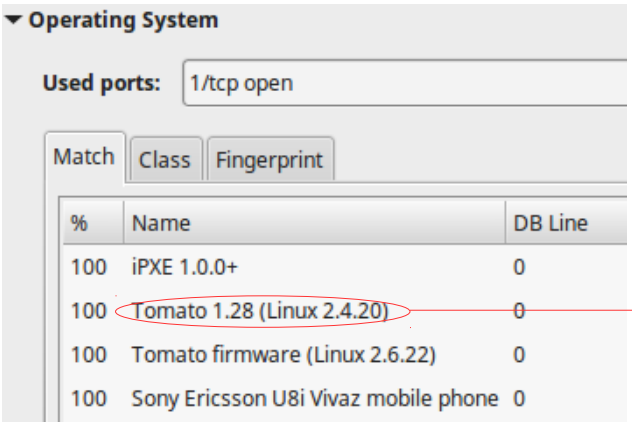




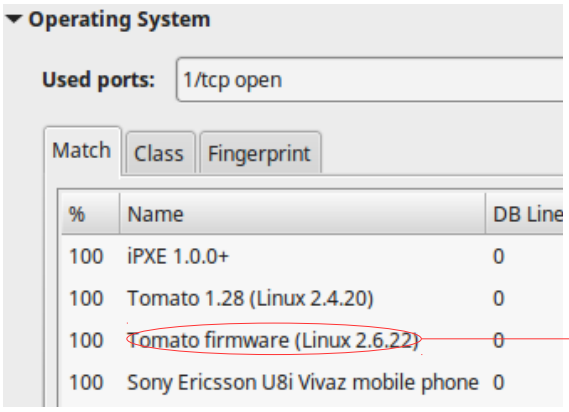
Tahap 3 : *Services* yang berjalan pada *host*

Port	Protocol	State	Service	Method
1	tcp	open	tcpmux	table
3	tcp	open	compressnet	table
4	tcp	open	unknown	table
6	tcp	open	unknown	table
7	tcp	open	echo	table
9	tcp	open	discard	table
13	tcp	open	daytime	table
17	tcp	open	qotd	table
19	tcp	open	chargen	table
20	tcp	open	ftp-data	table
21	tcp	open	tcpwrapped	probed
22	tcp	open	ssh	probed
23	tcp	open	telnet	table
24	tcp	open	priv-mail	table
25	tcp	open	smtp	table
26	tcp	open	rsftp	table
57797	tcp	open	unknown	table
58080	tcp	open	unknown	table
60020	tcp	open	unknown	table
60443	tcp	open	unknown	table
61532	tcp	open	unknown	table
61900	tcp	open	unknown	table
62078	tcp	open	iphone-sync	table
63331	tcp	open	unknown	table
64623	tcp	open	unknown	table
64680	tcp	open	unknown	table
65000	tcp	open	unknown	table
65129	tcp	open	unknown	table
65389	tcp	open	unknown	table

Tahap 4 : *vulnerabilities*



CVE-2003-0467	Unknown vulnerability in ip_nat_sack_adjust of Netfilter in Linux kernels 2.4.20, and some 2.5.x, when CONFIG_IP_NF_NAT_FTP or CONFIG_IP_NF_NAT_IRC is enabled, or the ip_nat_ftp or ip_nat_irc modules are loaded, allows remote attackers to cause a denial of service (crash) in systems using NAT, possibly due to an integer signedness error.
CVE-2003-0246	The ioperm system call in Linux kernel 2.4.20 and earlier does not properly restrict privileges, which allows local users to gain read or write access to certain I/O ports.
CVE-2003-0187	The connection tracking core of Netfilter for Linux 2.4.20, with CONFIG_IP_NF_CONNTRACK enabled or the ip_conntrack module loaded, allows remote attackers to cause a denial of service (resource consumption) due to an inconsistency with Linux 2.4.20's support of linked lists, which causes Netfilter to fail to identify connections with an UNCONFIRMED status and use large timeouts.
CVE-2002-1574	Buffer overflow in the ixj telephony card driver in Linux before 2.4.20 has unknown impact and attack vectors.
CVE-2002-1573	Unspecified vulnerability in the pcilynx ieee1394 firewire driver (pcilynx.c) in Linux kernel before 2.4.20 has unknown impact and attack vectors, related to "wrap handling."



CVE-2012-1583	Double free vulnerability in the xfrm6_tunnel_rcv function in net/ipv6/xfrm6_tunnel.c in the Linux kernel before 2.6.22, when the xfrm6_tunnel module is enabled, allows remote attackers to cause a denial of service (panic) via crafted IPv6 packets.
CVE-2008-5029	The __scm_destroy function in net/core/scm.c in the Linux kernel 2.6.27.4, 2.6.26, and earlier makes indirect recursive calls to itself through calls to the fput function, which allows local users to cause a denial of service (panic) via vectors related to sending an SCM_RIGHTS message through a UNIX domain socket and closing file descriptors.
CVE-2008-4210	fs/open.c in the Linux kernel before 2.6.22 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by creating an executable file in a setgid directory through the (1) truncate or (2) ftruncate function in conjunction with memory-mapped I/O.
CVE-2008-2931	The do_change_type function in fs/namespace.c in the Linux kernel before 2.6.22 does not verify that the caller has the CAP_SYS_ADMIN capability, which allows local users to gain privileges or cause a denial of service by modifying the properties of a mountpoint.
CVE-2008-2148	The utimensat system call (sys_utimensat) in Linux kernel 2.6.22 and other versions before 2.6.25.3 does not check file permissions when certain UTIME_NOW and UTIME_OMIT combinations are used, which allows local users to modify file times of arbitrary files, possibly leading to a denial of service.