Unit 1
Instalasi *Virtual Machine*

A. Tujuan

- Menyiapkan OS virtualisasi di PC sebagai penunjang kegiatan praktikum
- Mengimport *Virtual Machine* (VM) ke dalam *VirtualBox*

B. Latar Belakang

Kekuatan teknologi komputasi dan sumber daya komputer telah meningkat pesat selama 10 tahun terakhir salah satunya adalah teknologi virtualisasi. Hal ini membutuhkan prosesor *multicore* dan RAM dalam jumlah besar. Dengan virtualisasi, satu atau lebih komputer virtual dapat beroperasi di dalam satu komputer fisik. Komputer virtual yang berjalan di dalam komputer fisik disebut sebagai *Virtual Machine* (VM). VM ini sering disebut sebagai *guest* sedangkan komputer fisik sering disebut sebagai *host*.

C. Alat dan Bahan

- PC Host dengan minimal RAM 8 GB dan Hardisk 40 GB
- Koneksi Internet

D. Instruksi Kerja

1. Download dan Install VirtualBox

   Download master file sesuai sistem operasi yang digunakan melalui link http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html.

2. Download File Image VM

   Login terlebih dahulu **netacad.com**, kemudian klik https://netacad.com/portal/content/cyberops-associate-virtual-machines-vms

   Download file **cyberops_workstation.ova** dan **security_onion.ova**

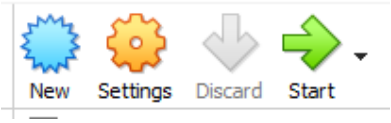
3. Import File VM ke VirtualBox

   Buka VirtualBox, klik File → Import Appliance

   Pilih file **.ova** yang telah didownload pada langkah sebelumnya.

4. Start VM

   Jalankan VM dengan klik tombol **start**.



Masukkan username dan password berikut:

Username : **analyst**

Password : **cyberops**

5. Mematikan VM

Ketikkan perintah **sudo shutdown -h now** pada terminal untuk mematikan VM.

6. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.

Unit 2
Eksplorasi Nmap

A. Tujuan

- Mengesplorasi Nmap
- Melakukan Scan ke Port yang terbuka

B. Latar Belakang

Port scanning biasanya merupakan bagian dari serangan pengintaian. Ada berbagai metode Port scanning yang dapat digunakan. Nmap adalah software jaringan yang digunakan untuk audit keamanan dengan menggunakan metode port scanning.

C. Alat dan Bahan

- CyberOps Workstation virtual machine
- Internet access

D. Instruksi Kerja

1. Eksplorasi Nmap
   Start CyberOps Workstation
   Buka terminal kemudian ketikkan

   [analyst@secOps ~]$ **man nmap**

   Apa itu Nmap?
   Apa fungsi dari Nmap?

2. *Localhost Scanning*

   [analyst@secOps ~]$ **nmap -A -T4 localhost**

   Starting Nmap 7.40 (https://nmap.org) at 2017-05-01 17:20 EDT
   Nmap scan report for localhost (127.0.0.1)
   Host is up (0.000056s latency).
   Other addresses for localhost (not scanned): ::1
   rDNS record for 127.0.0.1: localhost.localdomain
   Not shown: 996 closed ports
   PORT STATE SERVICE VERSION
   21/tcp open ftp vsftpd 2.0.8 or later
   | ftp-anon: Anonymous FTP login allowed (FTP code 230)
   |_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp_test
   <some output omitted>

   Port dan layanan apa yang terbuka?

Software apa yang digunakan pada port yang terbuka tersebut?

3. *Network Scanning*
   Sebelum melakukan scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu.

   [analyst@secOps ~]$ **ip address**
   <output omitted>
   2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
   valid_lft 85777sec preferred_lft 85777sec
   inet6 fe80::a00:27ff:feed:af2c/64 scope link
   valid_lft forever preferred_lft forever

   Berapakah alamat IP dan subnet mask dari PC host?

   Lakukanlah port scanning dengan menggunakan Nmap

   [analyst@secOps ~]$ **nmap -A -T4 10.0.2.0/24**

   Starting Nmap 7.40 (https://nmap.org) at 2017-05-01 17:13 EDT
   <output omitted>
   Nmap scan report for 10.0.2.15
   Host is up (0.00019s latency).
   Not shown: 997 closed ports
   PORT STATE SERVICE VERSION
   21/tcp open ftp vsftpd 2.0.8 or later
   | ftp-anon: Anonymous FTP login allowed (FTP code 230)
   |_-rw-r--r-- 1 0 0 0 Mar 26 2018 ftp_test
   | ftp-syst:
   | STAT:
   | FTP server status:
   | Connected to 10.0.2.15
   | Logged in as ftp
   | TYPE: ASCII
   | No session bandwidth limit
   | Session timeout in seconds is 300

```
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0)
23/tcp open  telnet  Openwall GNU/*/Linux telnetd
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Post-scan script results:
| clock-skew:
|   0s:
|     10.0.2.4
|     10.0.2.3
|_    10.0.2.2
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds
```

Berapakah jumlah host yang terdeteksi?

4. *Remote Server Scanning*
   Buka web browser dan kunjungi **scanme.nmap.org**
   Ketikkan perintah berikut:

```
[analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
```

25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
4444/tcp filtered krb524
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds

Port dan layanan apa yang terbuka?

Berapa alamat IP server?

Apa sistem operasi yang digunakan oleh server?

5. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.