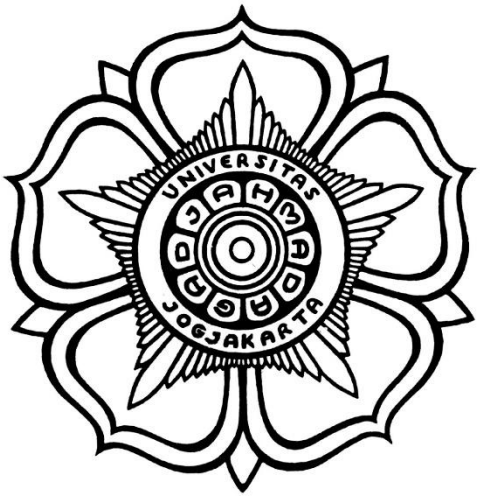
LAPORAN PRATIKUM
KEAMANAN INFORMASI 1
UNIT 2



Disusun Oleh :

NAMA : Riva Mahyuli
NIM :21/478709/SV/19365
KELAS :R1AA
DOSEN : Anni Karimatul Fauziyyah,S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS GADJAH MADA
2022/2023

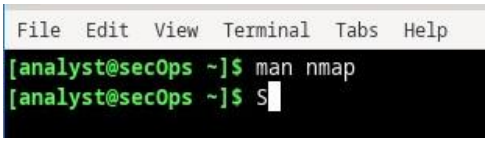
UNIT 2
Eksplorasi Nmap

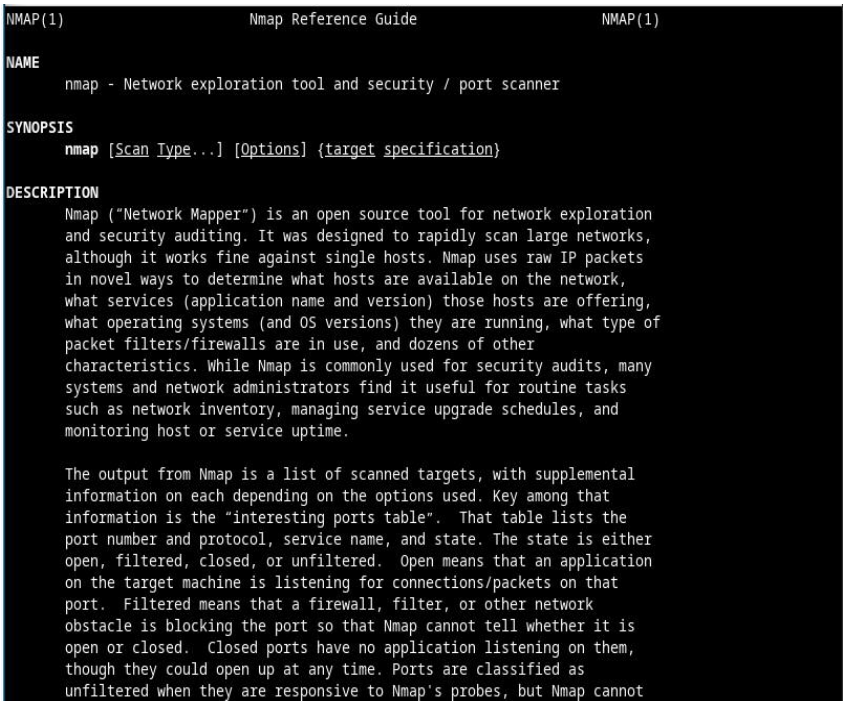
A. Alat dan Bahan

- CyberOps Workstation virtual machine
- Internet access

C. Langkah kerja

1. Eksplorasi Nmap, ***[analyst@secOps ~]$ man nmap***





2. Localhost Scanning, ***[analyst@secOps ~]$ nmap -A -T4 localhost***

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:49 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
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 127.0.0.1
|      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 2
|      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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.10 seconds
```

3. Network scanning, ***[analyst@secOps ~]$ ip address***

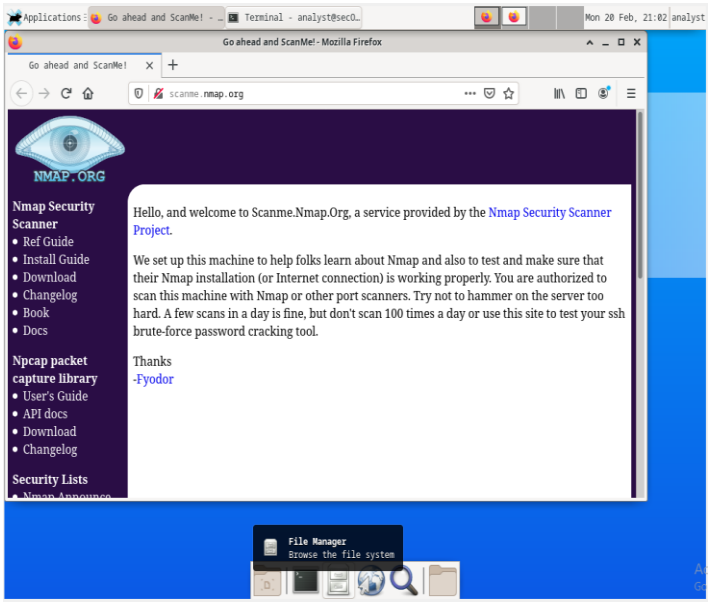
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
    link/ether 08:00:27:3d:19:2b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 84938sec preferred_lft 84938sec
    inet6 fe80::a00:27ff:fe3d:192b/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

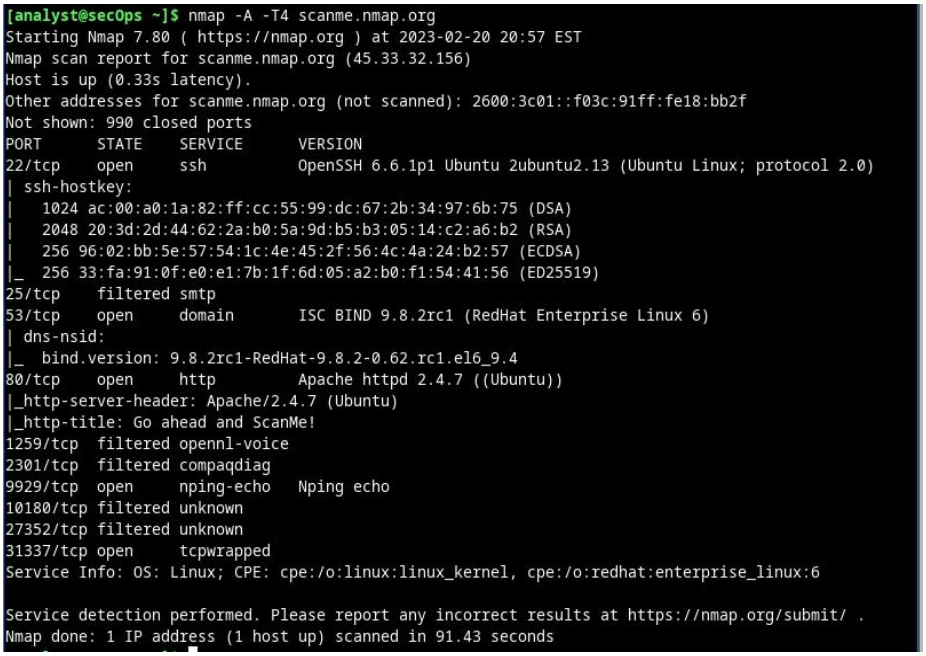
analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:01 EST
Nmap scan report for 10.0.2.15
Host is up (0.00015s 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 4
|      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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 44.87 seconds
```

4. Remote server scanning, buka scanme.nmap.org di web cybercops workstation, lalu ketikan perintah syntax di terminal





UNIT 3

Pemantauan Trafik HTTP dan HTTPS
dengan menggunakan Wireshark

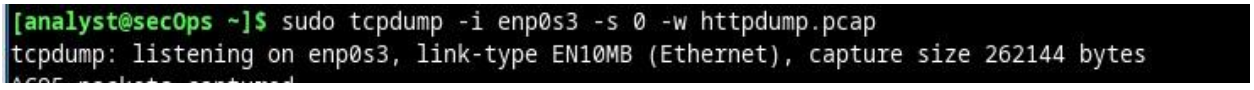
A. Alat dan Bahan

- CyberOps Workstation VM
- Koneksi Internet

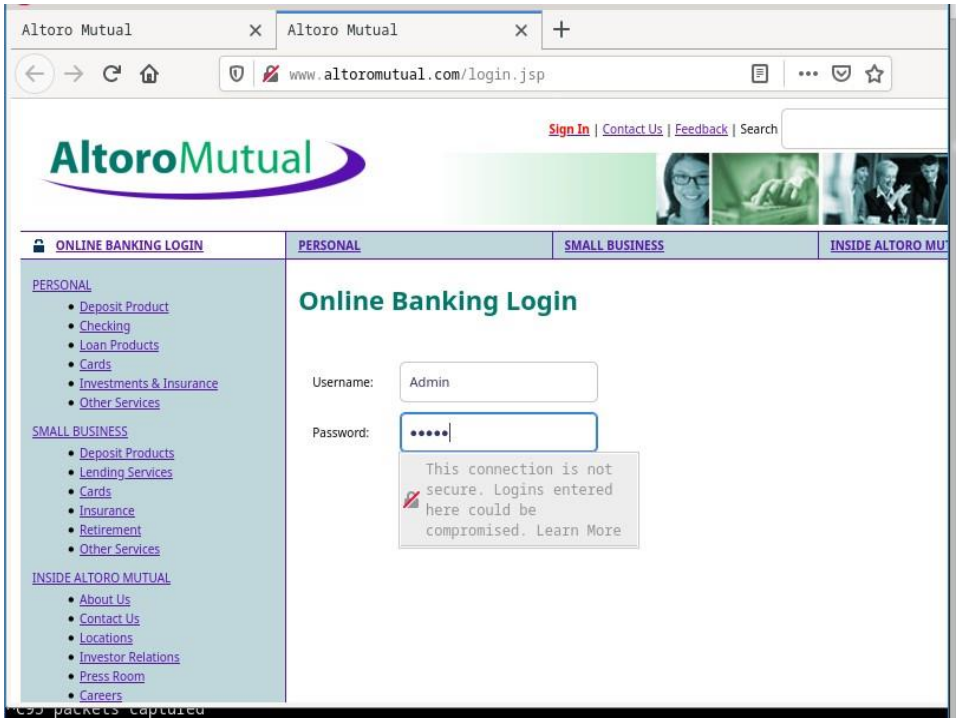
C.Langkah Kerja

1. Buka VM dan jalankan cybercops workstation,lalu login dengan Username: analyst, Password: cyberops

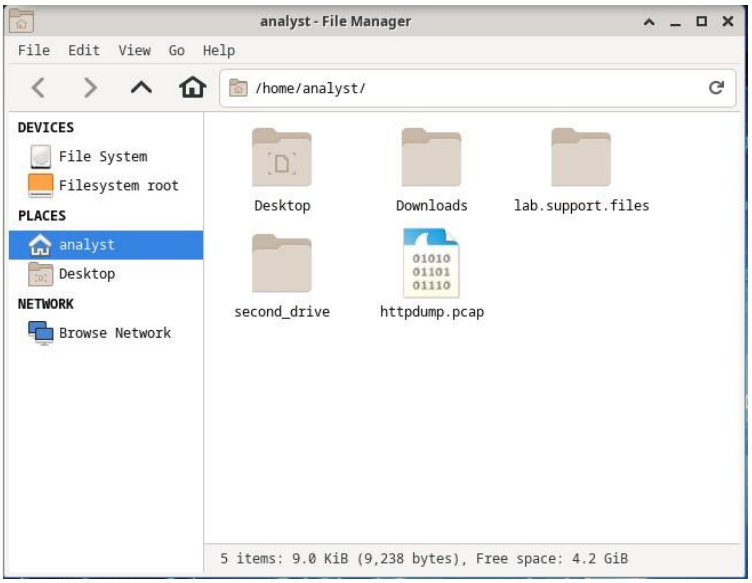
2. Buka terminal dan menjalankan tcpdump dan pengecekan alamat IP dengan menggunakan perintah:
[analyst@secOps ~]$ ip address
[analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap



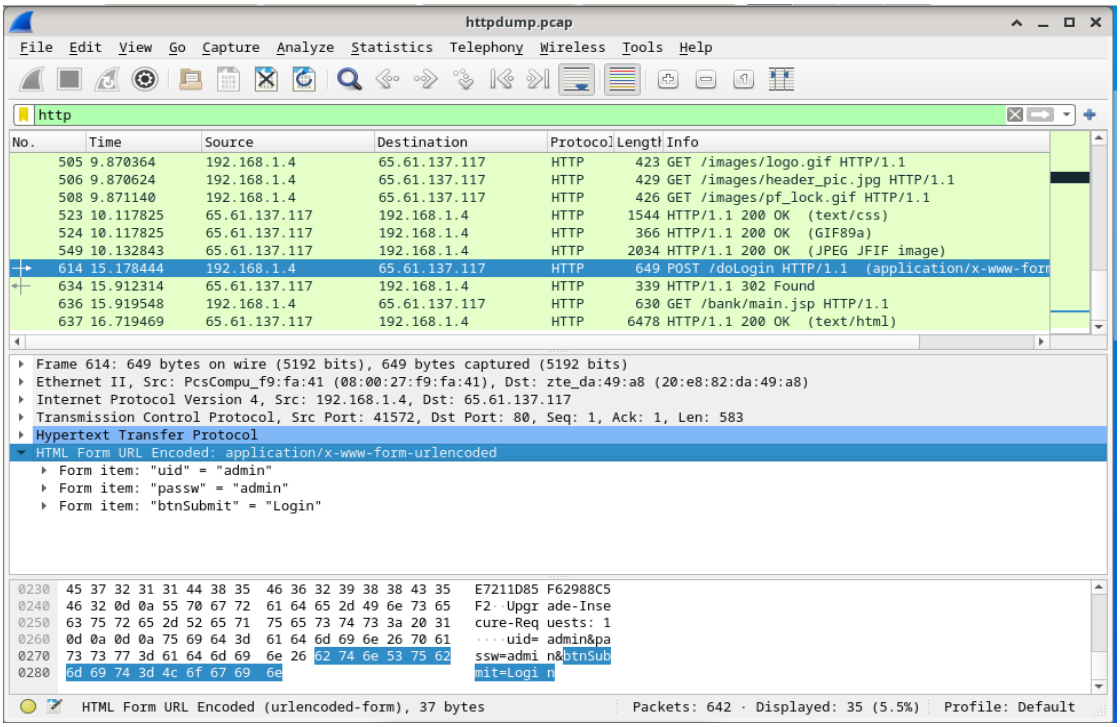
3. Buka link http://www.altoromutual.com/login.jsp melalui browser di CyberOps Workstation VM.
Username : Admin
Password : Admin



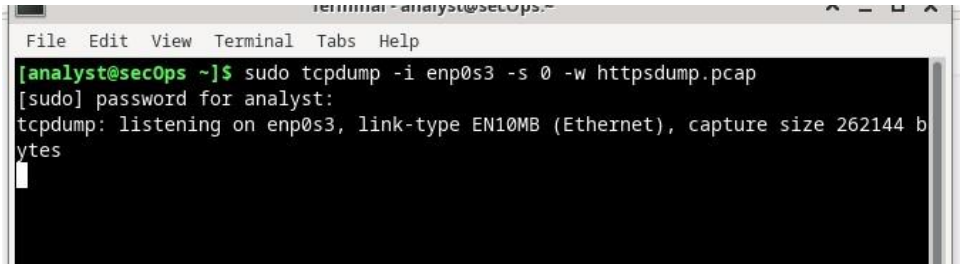
4. Merekam Paket HTTP Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



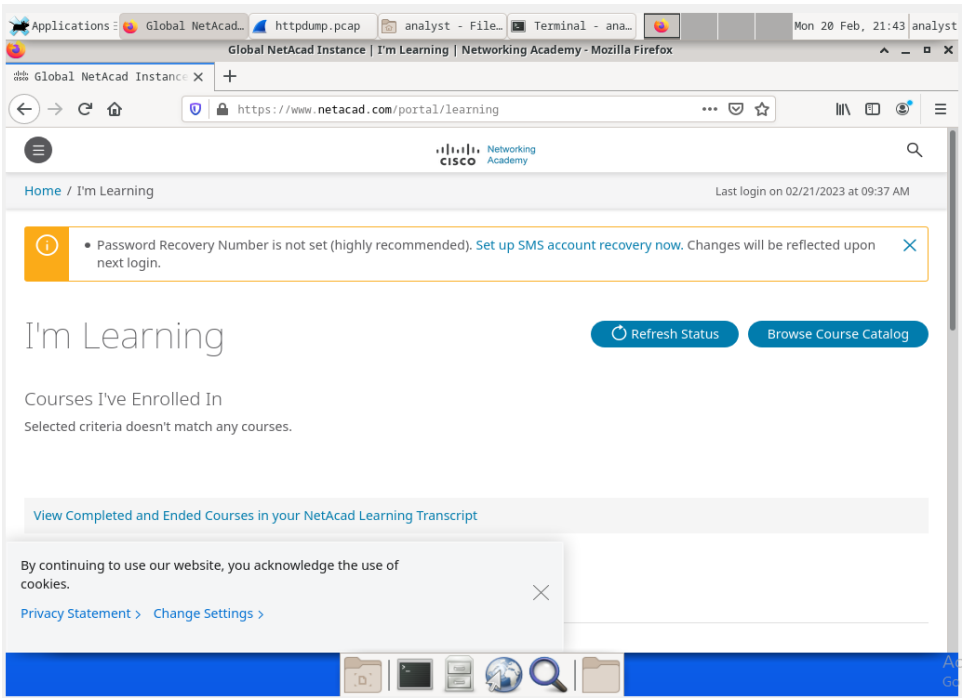
5.Buka wireshark dan tuliskan di filter HTTP kemudian klik apply lalu pilih POST



6. Merekam paket HTTPS



7. Buka link netacad melalui browser di CyberOps Workstation VM dan login mengunakan akun pribadi.



7. Melihat rekaman paket HTTP