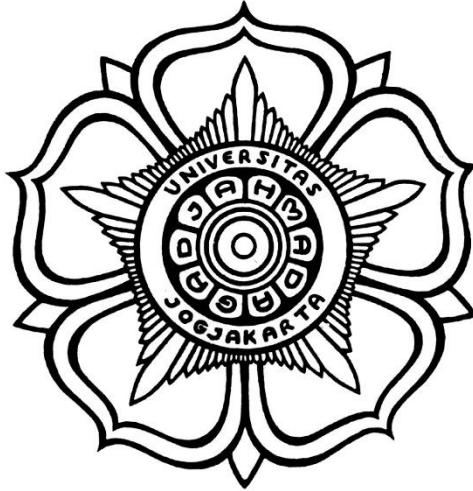


**LAPORAN PRATIKUM
KEAMANAN INFORMASI 1
UNIT 2**



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*

```
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ S
```

```
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    information is the "interesting ports table". That table lists the
    port number and protocol, service name, and state. The state is either
    open, filtered, closed, or unfiltered. Open means that an application
    on the target machine is listening for connections/packets on that
    port. Filtered means that a firewall, filter, or other network
    obstacle is blocking the port so that Nmap cannot tell whether it is
    open or closed. Closed ports have no application listening on them,
    though they could open up at any time. Ports are classified as
    unfiltered when they are responsive to Nmap's probes, but Nmap cannot
```

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)
|_IW-I--I-- 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*

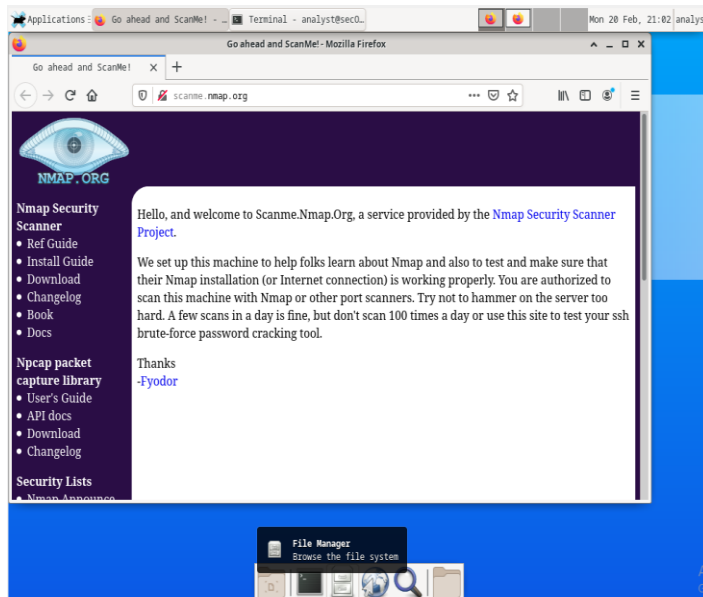
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    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 ketikkan perintah syntax di terminal



```

[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:57 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (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)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
53/tcp    open  domain       ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
|_ dns-nsid:
|_ bind.version: 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.4
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
1259/tcp  filtered openssl-voice
2301/tcp  filtered compaqdiag
9929/tcp  open  nping-echo   Nping echo
10180/tcp filtered unknown
27352/tcp filtered unknown
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel, cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.43 seconds

```

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
```

```

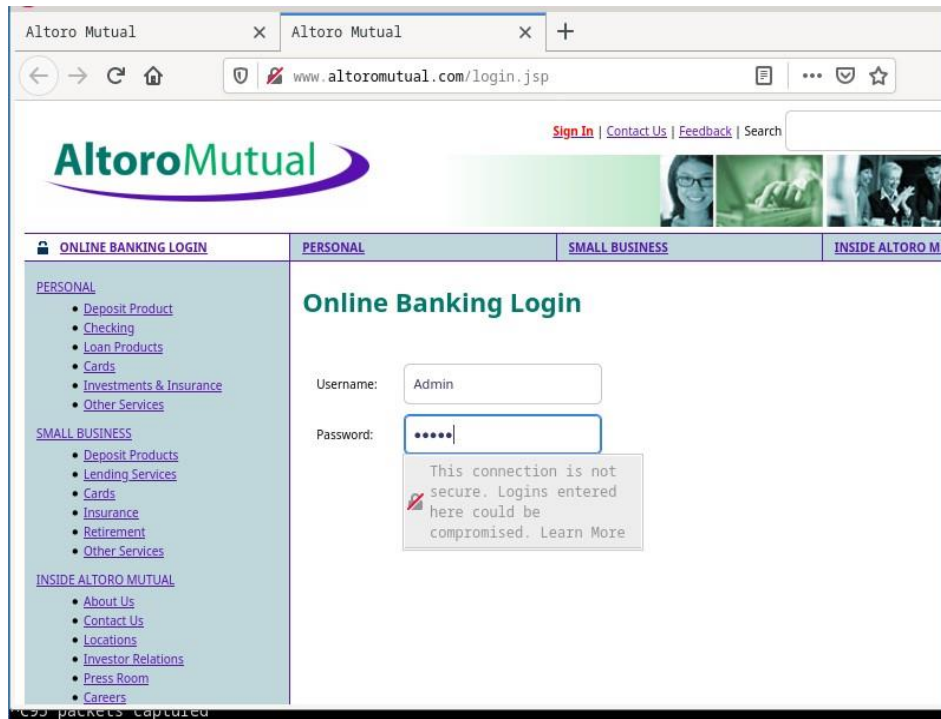
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C

```

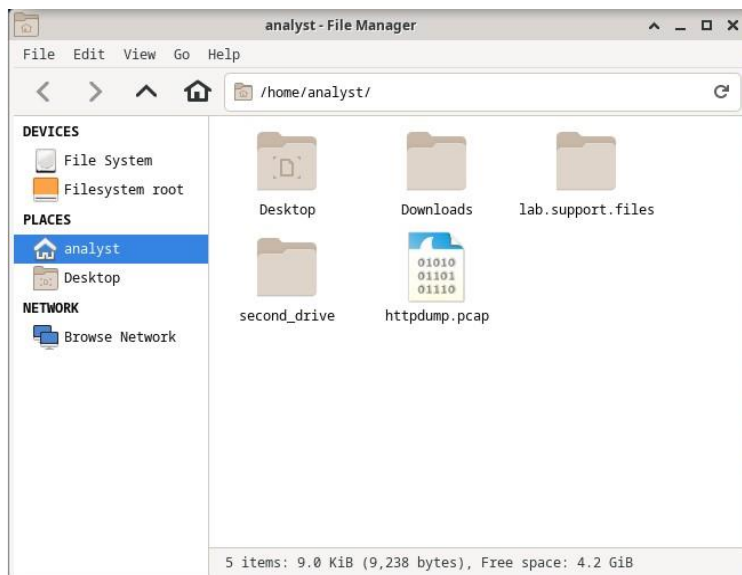
3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM.

Username : Admin

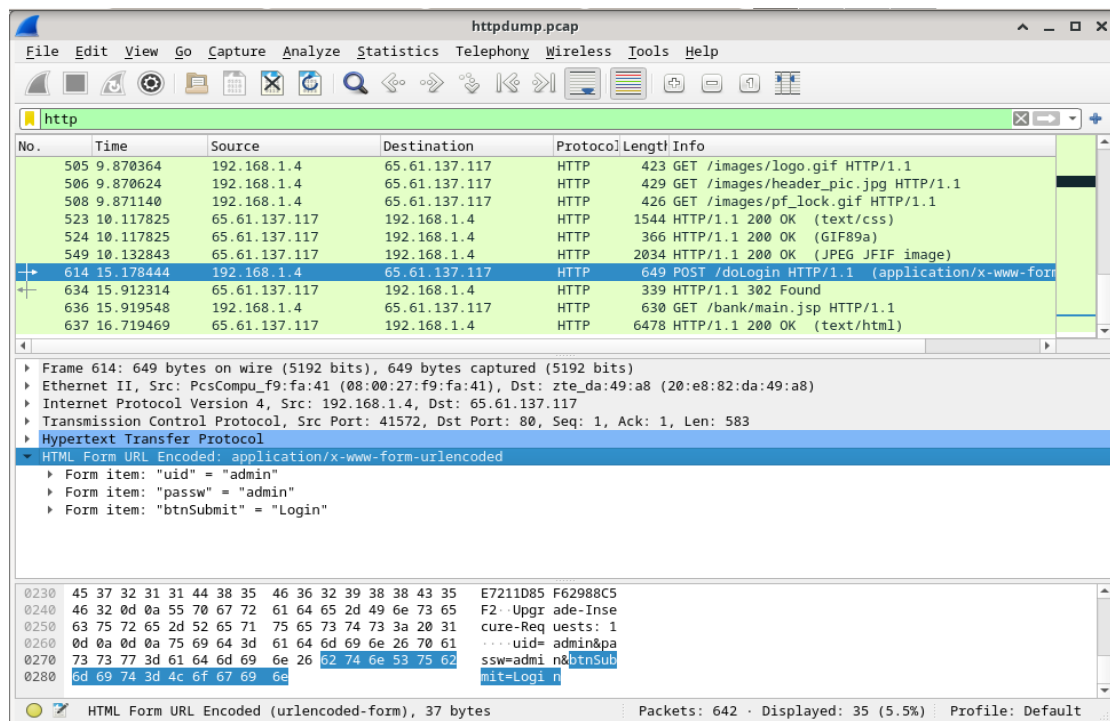
Password : Admin



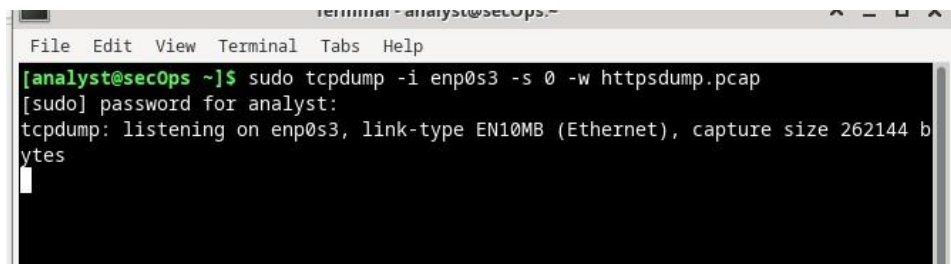
4. Merekam Paket HTTP Tcpcdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



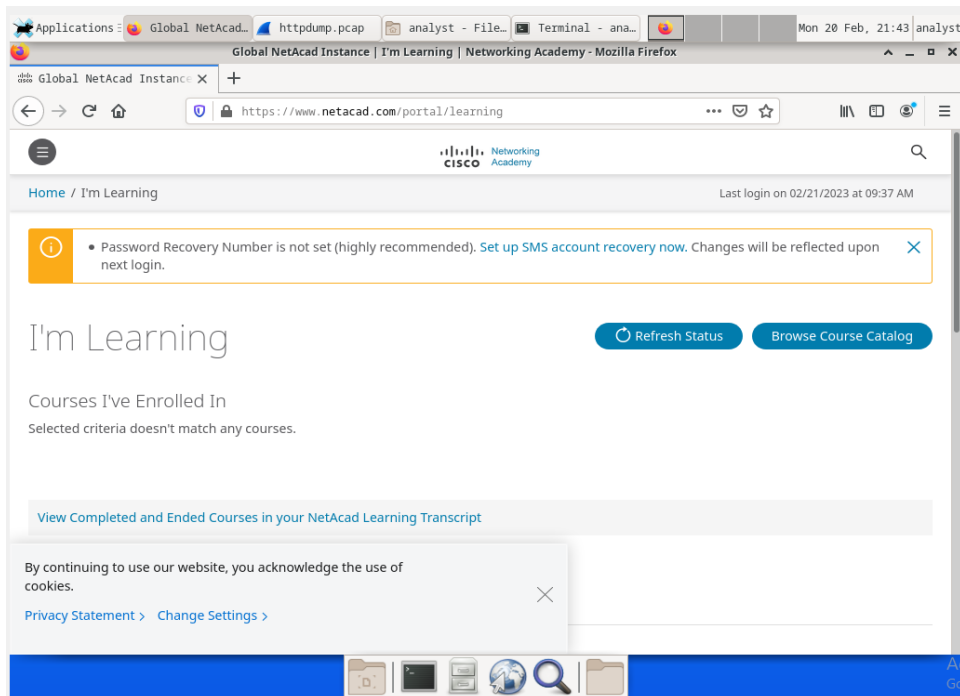
5. Buka wireshark dan tuliskan di filter HTTP kemudian klik apply lalu pilih POST



6. Merekam paket HTTPS



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



7. Melihat rekaman paket HTTP

