

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
EKSPLORASI NMAP DAN PEMANTAUAN TRAFIK
HTTP DAN HTTPs MENGGUNAKAN WIRESHARK



DISUSUN OLEH

Nama : Fariansyah Permata Surya
NIM : 21/473155/SV/18810
Hari, Tanggal : Minggu, 27/02/2023
Kelas : RI4AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA

2022

A. Dasar Teori

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.

HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi.

Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan arti sebenarnya dari data yang sedang dipertukarkan. Hal ini dilakukan melalui penggunaan sertifikat yang dapat dilihat nanti di lab ini.

Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

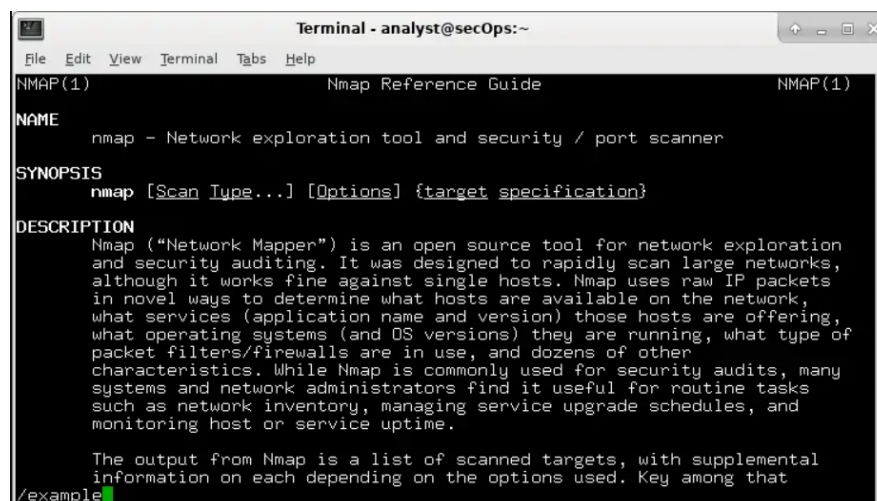
B. Alat dan Bahan

1. PC Host dengan minimal RAM 8 GB dan Hardisk 40 GB
2. Koneksi Internet
3. CyberOps Workstation VM

C. Tugas dan Penyelesaian

Unit 2

1. Jalankan CyberOps Workstation VM pada VirtualBox. Setelah memasukkan User dan Password, buka terminal CyberOps Workstation VM kemudian ketikkan perintah “man nmap”.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
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
/example
```

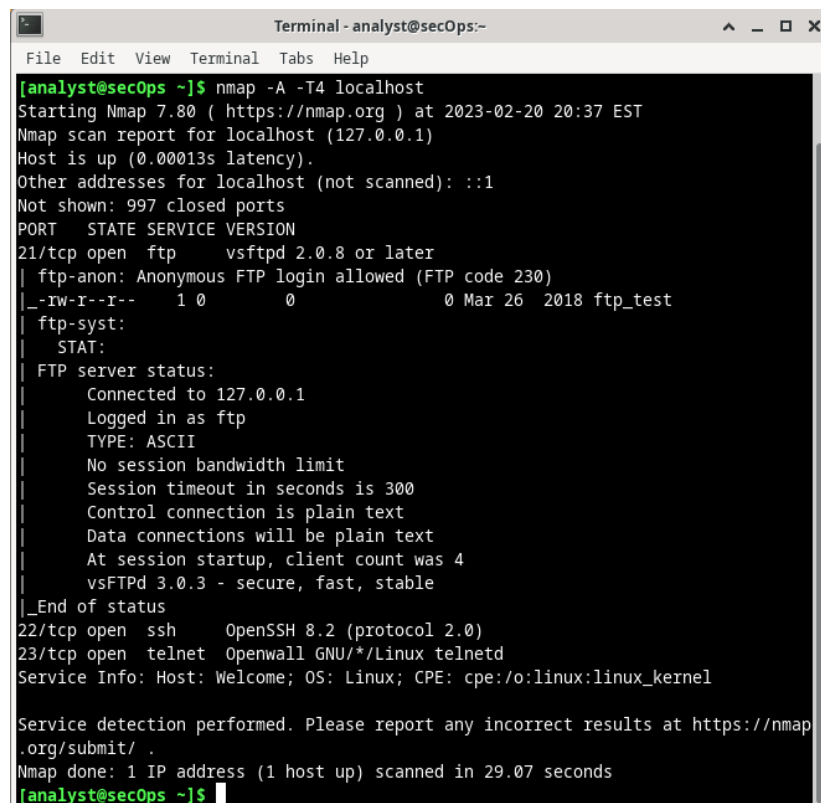
- Apa itu Nmap?

Jawab : Nmap adalah alat eksplorasi jaringan dan pemindai keamanan / port.

- Apa fungsi dari Nmap?

Jawab : Nmap digunakan untuk memindai jaringan dan menentukan host yang tersedia dan layanan yang ditawarkan di jaringan. Beberapa fitur nmap termasuk penemuan host, pemindaian port, dan deteksi sistem operasi. Nmap dapat digunakan secara umum untuk audit keamanan, untuk mengidentifikasi port terbuka, inventaris jaringan, dan menemukan kerentanan dalam jaringan.

2. Kemudian lakukan local host scanning dengan mengetikkan perintah “nmap -A -T4 localhost”.



```

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:37 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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 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: 1 IP address (1 host up) scanned in 29.07 seconds
[analyst@secOps ~]$

```

- Port dan layanan apa yang terbuka?

Jawab : 21/tcp: ftp, 22/tcp: ssh, 23/tcp: telnet.

- Software apa yang digunakan pada port yang terbuka tersebut?

Jawab : ftp : vsftpd, ssh : OpenSSH, telnet : Openwall GNU/Linux telnetd.

3. Selanjutnya adalah melakukan network scanning dimana sebelum melakukan scanning lakukan perintah “ip address” untuk mengetahui alamat IP host terlebih dahulu.

```
[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 08:00:27:06:b9:3a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 82297sec preferred_lft 82297sec
    inet6 fe80::a00:27ff:fe06:b93a/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

- Berapakah alamat IP dan subnet mask dari PC host?

Jawab : IP address = 10.0.2.15/24 dan subnet mask = 255.255.255.0.

4. Lakukanlah port scanning dengan menggunakan Nmap dengan perintah “nmap -A -T4 10.0.2.0/24”.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
    valid_lft forever preferred_lft forever
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:42 EST
Nmap scan report for 10.0.2.15
Host is up (0.00014s 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 3
|   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

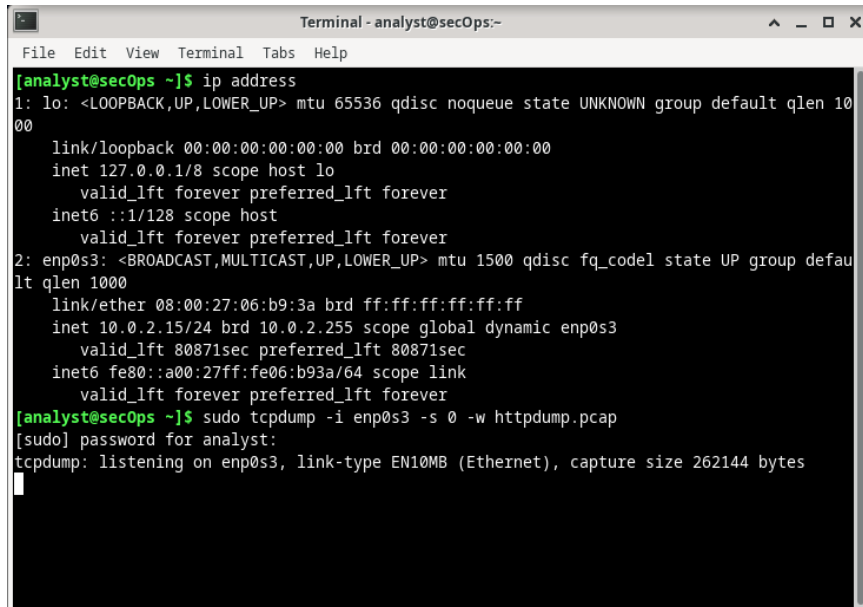
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 44.76 seconds
[analyst@secOps ~]$
```

- Berapakah jumlah host yang terdeteksi?

Jawab : 1 host.

Unit 3

1. Jalankan CyberOps Workstation VM pada VirtualBox. Setelah memasukkan User dan Password, buka terminal CyberOps Workstation VM kemudian ketikkan perintah “ip address” untuk mengecek alamat IP, kemudian ketik perintah “sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap”.

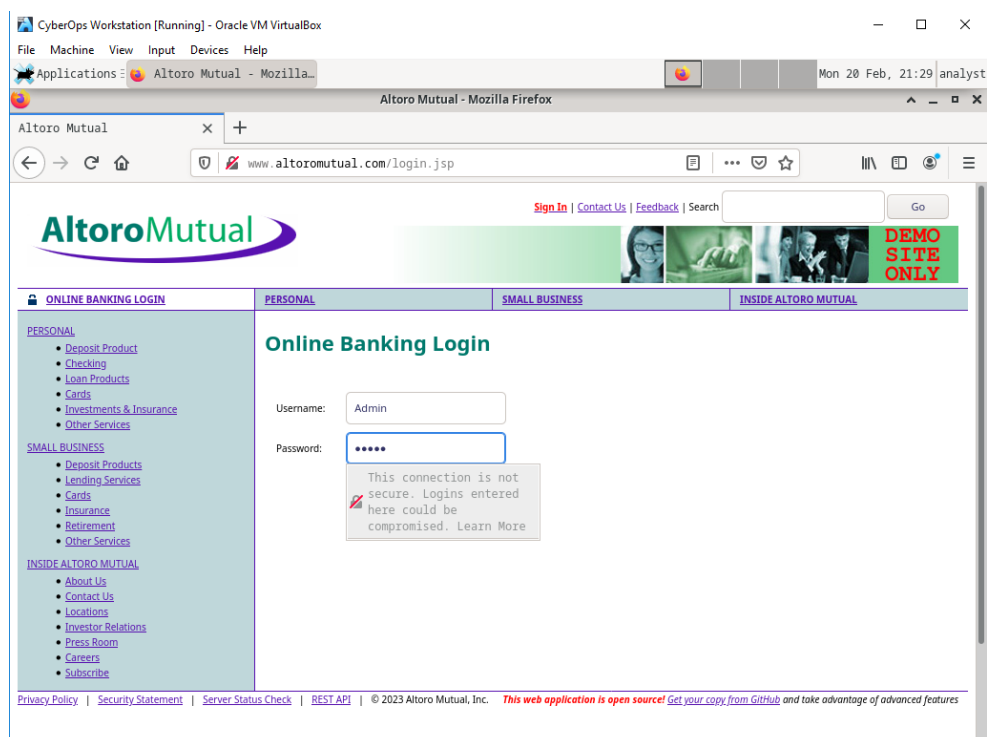


```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

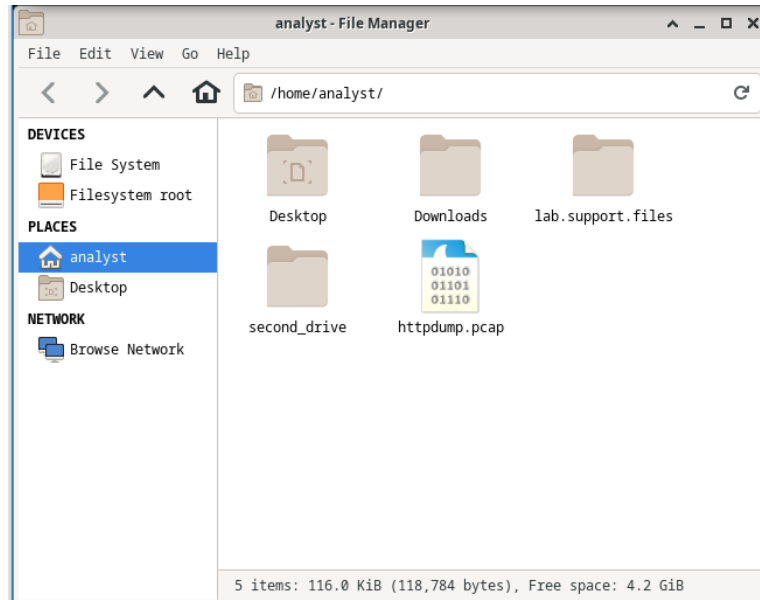
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        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 08:00:27:06:b9:3a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 80871sec preferred_lft 80871sec
    inet6 fe80::a00:27ff:fe06:b93a/64 scope link
        valid_lft forever preferred_lft forever

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

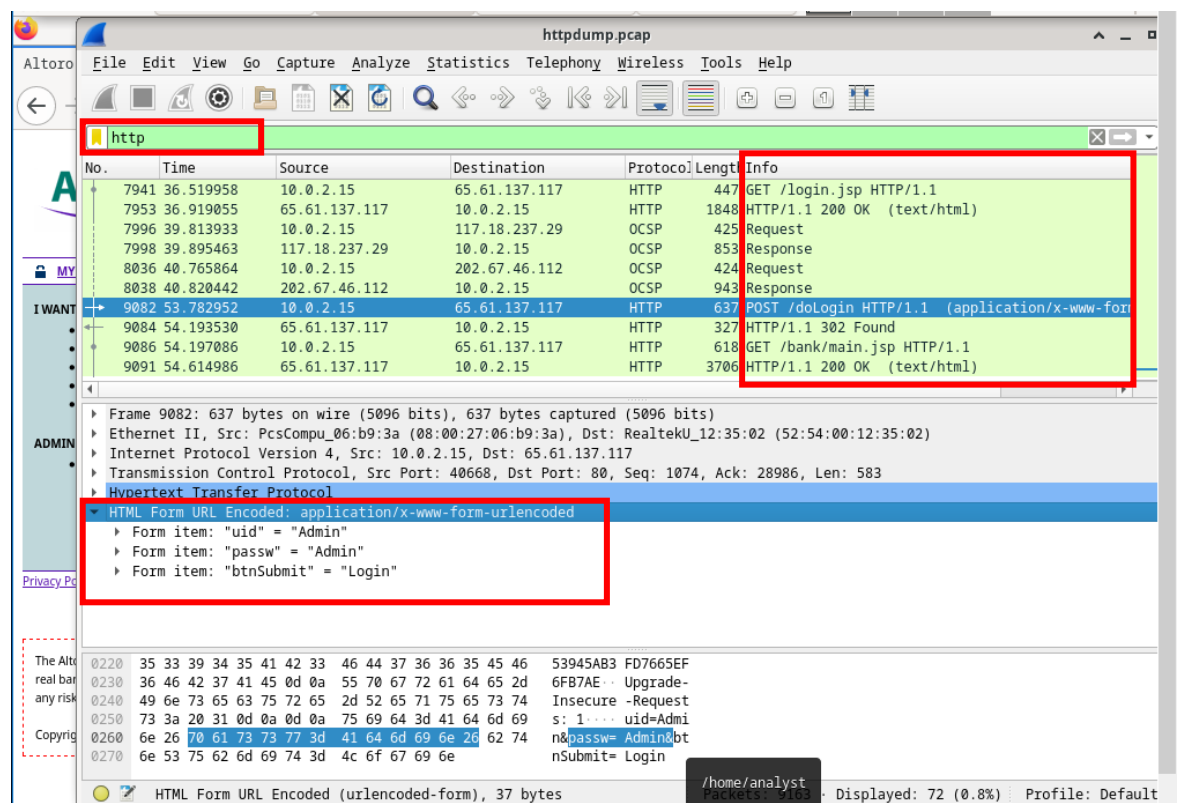
2. Buka browser kemudian masuk ke link <http://www.altoromutual.com/login.jsp>. Masukkan Username : Admin dan Password : Admin.



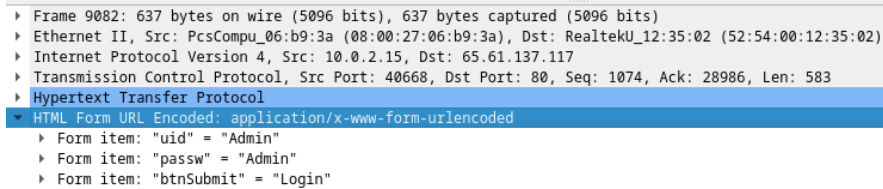
3. Tcpcap yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/. File httpdump.pcap akan merekam paket HTTP.



4. Import file httpdump.pcap pada aplikasi wireshark. Lakukan filter "http" kemudian pilih POST pada bagian Info lalu klik 2 kali pada bagian HTML Form URL Encoded.

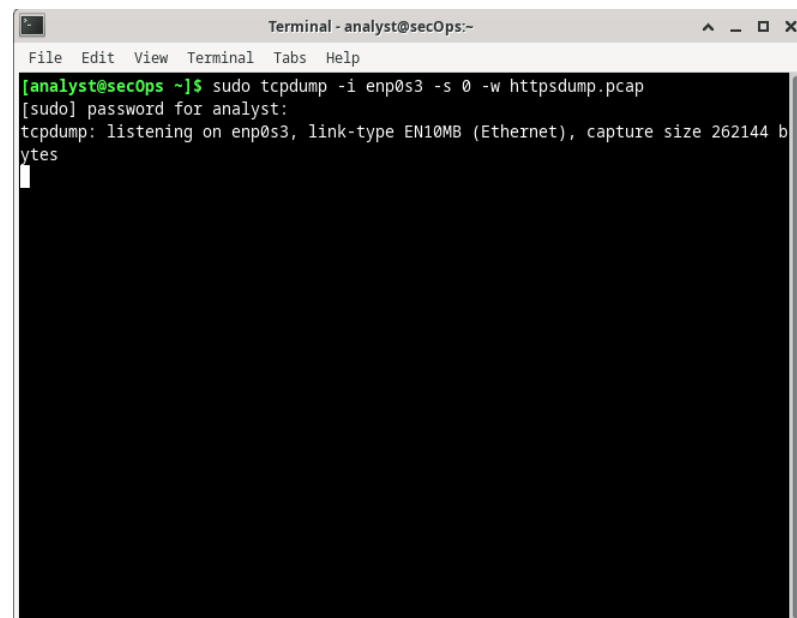


5. Berdasarkan gambar diatas pada Website HTTP terlihat langsung bahwa saat pada login di website HTTP informasi username dan password terekam dengan jelas sesuai dengan yang dilakukan pada saat login sebelumnya.



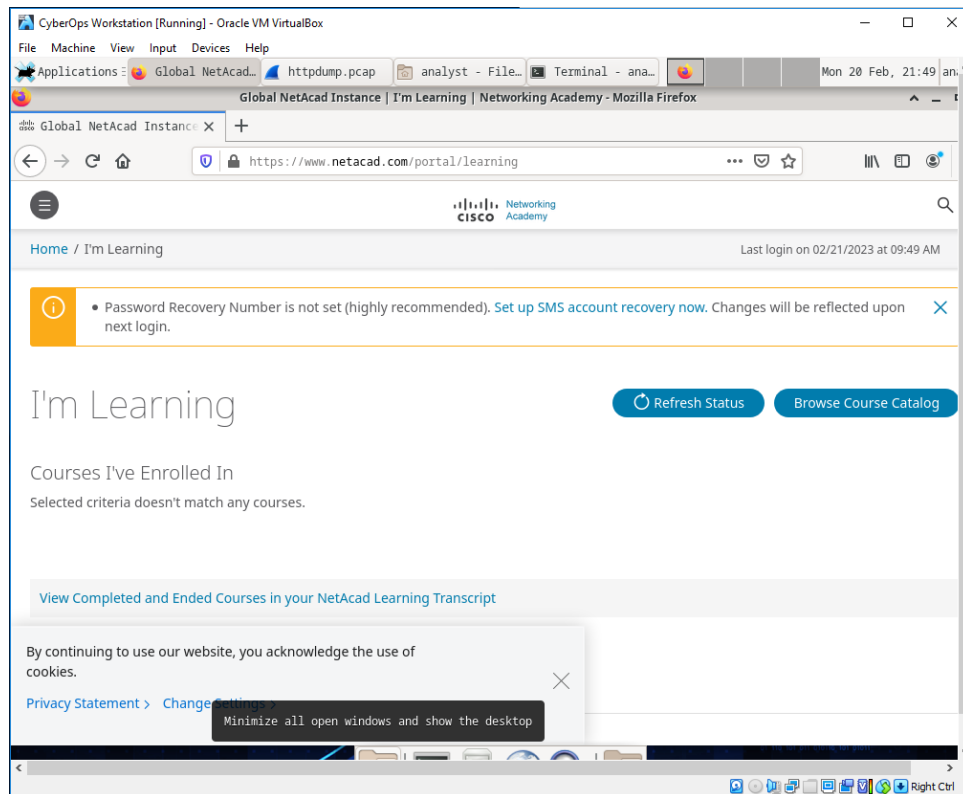
```
Frame 9082: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface 0  
Ethernet II, Src: PcsCompu_06:b9:3a (08:00:27:06:b9:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117  
Transmission Control Protocol, Src Port: 40668, Dst Port: 80, Seq: 1074, Ack: 28986, Len: 583  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded  
Form item: "uid" = "Admin"  
Form item: "passw" = "Admin"  
Form item: "btnSubmit" = "Login"
```

6. Kemudian lakukan perintah “`sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`” pada terminal dan sama seperti sebelumnya dimana file bernama `httpsdump.pcap` akan tersimpan pada folder `/home/analyst/`.

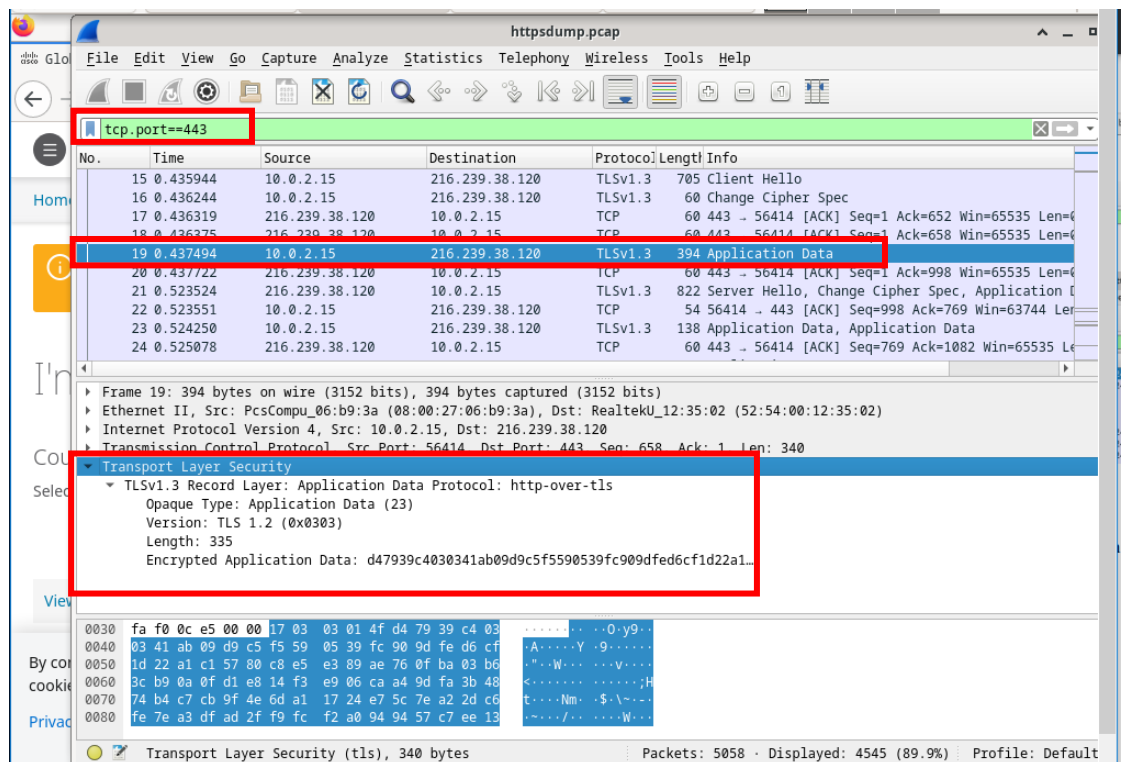


```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap  
[sudo] password for analyst:  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

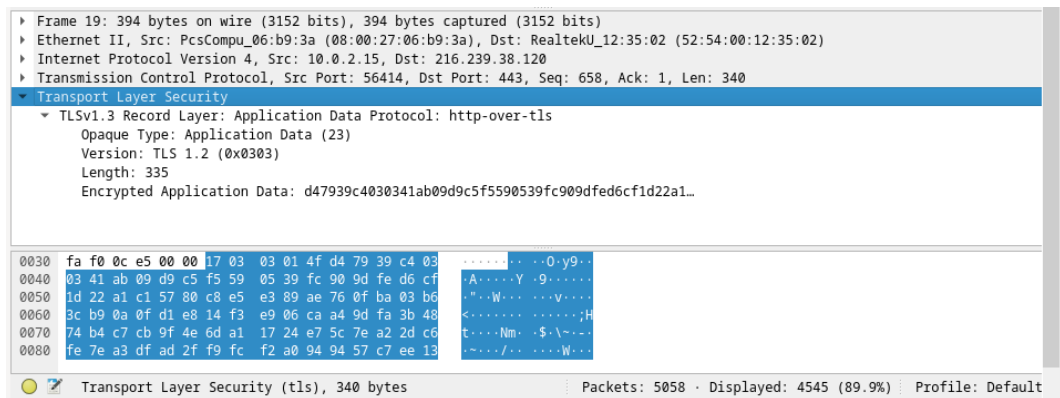
7. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM dan lakukan login pada website netacad menggunakan akun cisco.



8. Kemudian import file httpdump.pcap pada aplikasi wireshark. Lakukan filter “tcp.port==443” kemudian pilih Application Data dan klik 2 kali pada bagian Transport Layer Security.



9. Berdasarkan gambar diatas pada Website HTTPs terlihat berbeda dengan pada Website HTTP dimana pada Website HTTPs datanya ter enkripsi sehingga informasi tentang username dan password saat login tidak terlihat langsung tidak seperti Website HTTP sebelumnya dimana informasi login terlihat langsung.



D. Analisis

Pada praktikum Keamanan Informasi 1 pertemuan 2 membahas mengenai Nmap serta perbedaan Website HTTP dengan Website HTTPs dengan menggunakan wireshark. Pada praktikum kali ini menggunakan 2 buah tools software yaitu nmap dan wireshark. Nmap adalah sebuah perangkat lunak open source (gratis dan dapat diakses oleh siapa saja) yang digunakan untuk melakukan pemindaian jaringan dan pengujian keamanan. Nmap digunakan untuk memetakan jaringan, mengetahui informasi tentang host dan servis, dan menemukan celah keamanan dalam jaringan sedangkan Wireshark adalah sebuah perangkat lunak open source (gratis dan dapat diakses oleh siapa saja) yang digunakan untuk menganalisis lalu lintas jaringan. Wireshark memungkinkan pengguna untuk menangkap, menganalisis, dan memecahkan paket data yang dikirimkan melalui jaringan computer.

Pada unit 2 dilakukan pengekplorasi nmap dimana saat melakukan port scanning atau network scanning dibutuhkan alamat IP sebagai tujuan untuk scanning. Perintah yang digunakan adalah -T4 untuk eksekusi lebih cepat dengan melarang penundaan pemindaian dinamis melebihi 10 ms untuk port TCP. -T4 direkomendasikan untuk koneksi broadband atau ethernet yang layak. Sedangkan -A untuk mengaktifkan deteksi OS, deteksi versi, pemindaian skrip, dan traceroute. Hal yang didapat saat menggunakan nmap adalah seperti

port dan layanan terbuka serta software yang digunakan pada port dan layanan tersebut dan juga jumlah host yang aktif.

Dan pada unit 3 dilakukan perbandingan traffic paket HTTP dengan HTTPSs menggunakan Wireshark. Hasil yang didapat adalah Website dengan protokol HTTPSs lebih aman dibandingkan dengan Website dengan protokol HTTP dimana data pada Website HTTPSs datanya terenkripsi sehingga tidak dapat langsung menampilkan username dan password saat login, sedangkan Website HTTP langsung menampilkan informasi berupa username dan password saat login.

E. Kesimpulan

Berdasarkan data diatas dapat disimpulkan bahwa tools Nmap serta Wireshark digunakan untuk mencari celah keamanan pada jaringan sehingga dapat memperbaiki serta menjaga keamanan pada celah jaringan tersebut.

Dan juga perbedaan antara HTTP dan HTTPS adalah HTTP dapat dikatakan sebagai protokol standar dan HTTPS adalah pengembangan yang lebih aman dan terenkripsi. Penting untuk dicatat bahwa HTTPS lebih disukai daripada HTTP, terutama untuk situs web yang mengumpulkan atau memproses data sensitive karena datanya terenkripsi.

F. Daftar Pustaka

1. Pengertian NMAP Adalah : Fungsi, Cara Kerja & Penggunaannya. (n.d.). Wwww.nesabamedia.com. <https://www.nesabamedia.com/pengertian-nmap/>
2. Pengertian Wireshark : Fungsi dan Cara kerjanya (Lengkap). (n.d.). Wwww.nesabamedia.com. <https://www.nesabamedia.com/pengertian-wireshark/>
3. Intern, D. (2020, June 23). Apa Perbedaan HTTP dan HTTPS? Lengkap Beserta Penjelasan. Dicoding Blog. <https://www.dicoding.com/blog/perbedaan-http-dan-https/>