

**LAPORAN PRAKTIKUM
KEAMANAN INFORMASI I
PERTEMUAN KEDUA
PEMANTAUAN TRAFIK HTTP DAN HTTPS DENGAN
MENGUNAKAN WIRESHARK**



DI SUSUN OLEH

Nama : Faizal Ilyas Syah Putra
NIM : 21/474428/SV/18920
Kelas : RI1AA

**LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

A. LANDASAN TEORI

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 dipercayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

Wireshark berguna untuk pekerjaan analisis jaringan. Aplikasi ini umum digunakan sebagai alat troubleshoot pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk pengujian software karena kemampuannya untuk membaca konten dari tiap paket trafik data.

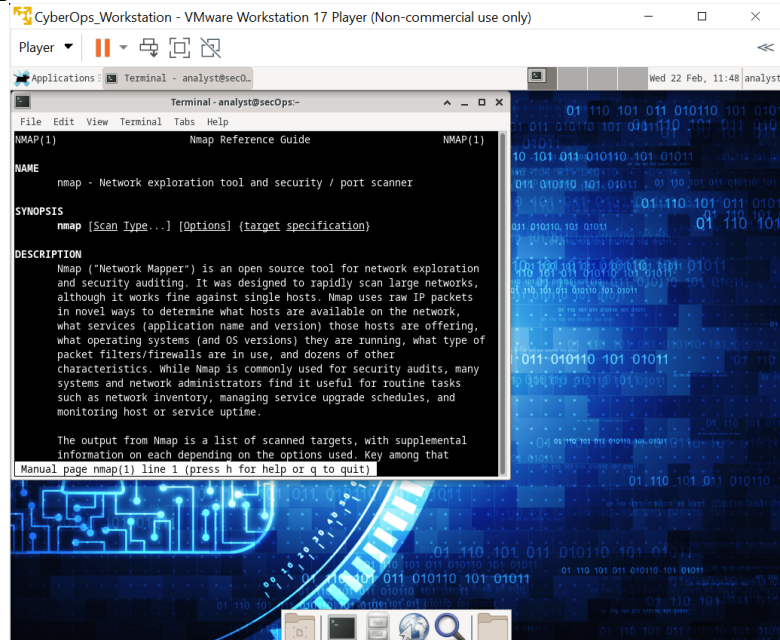
Agar dapat bekerja dengan baik, Wireshark membutuhkan aplikasi bernama WinPcap atau Npcap sebagai pondasinya. WinPcap masih dapat digunakan sampai versi Windows 7, sedang untuk Windows 10 sudah tidak didukung lagi, seterusnya sudah dikembangkan Npcap. Berbeda dengan pcap sebagai libcap library pada sistem Linux, Windows hanya menggunakan sebuah port saja dari library libcap tersebut yaitu Npcap.

B. PERCOBAAN DAN HASIL PRAKTIKUM

Unit 2 Eksplorasi Nmap

1. Ekspolarsi Nmap

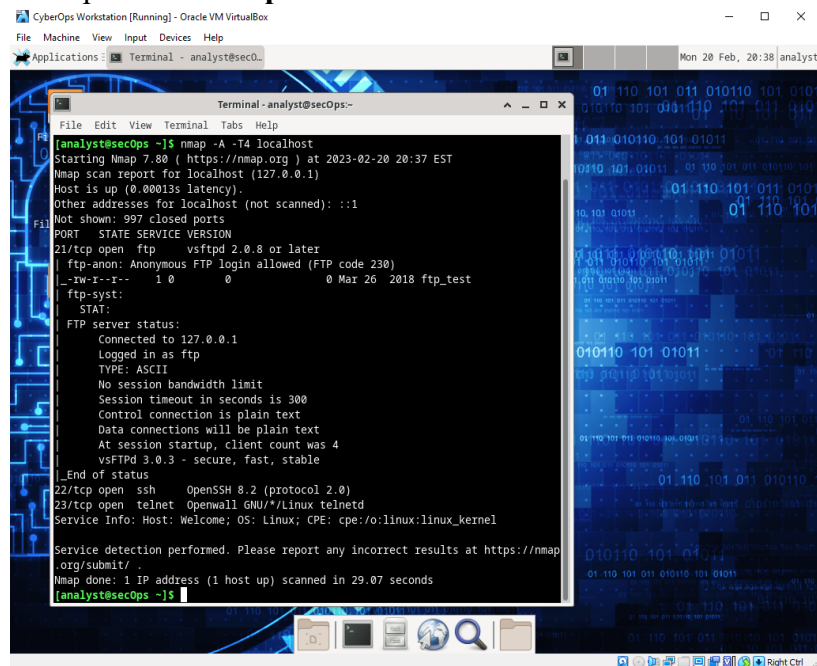
Buka CyberOps Workstation → masuk terminal dan ketikkan **man nmap**



```
CyberOps_Workstation - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications: Terminal - analyst@secOps--
Terminal - analyst@secOps--
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
Manual page nmap(1) line 1 (press h for help or q to quit)
```

2. Localhost Scanning

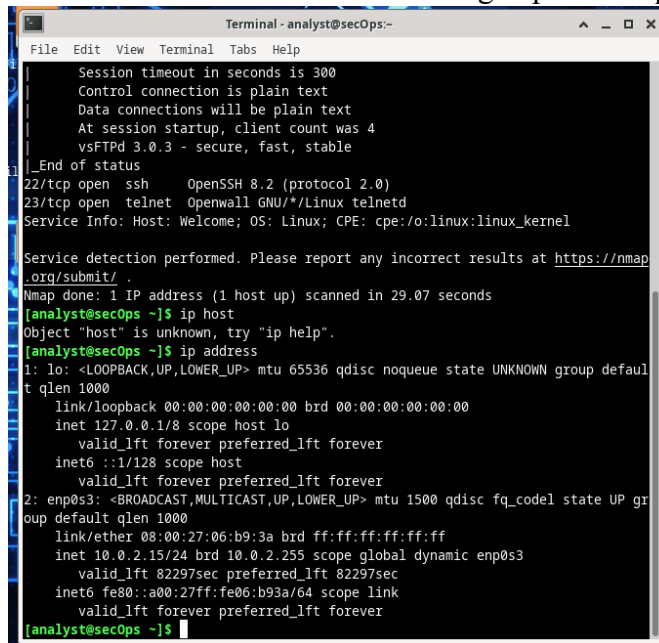
Ketikkan perintah **nmap -A -T4 localhost**



```
CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications: Terminal - analyst@secOps--
Terminal - analyst@secOps--
[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)
|_ftp-r--w-- 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 ~]$
```

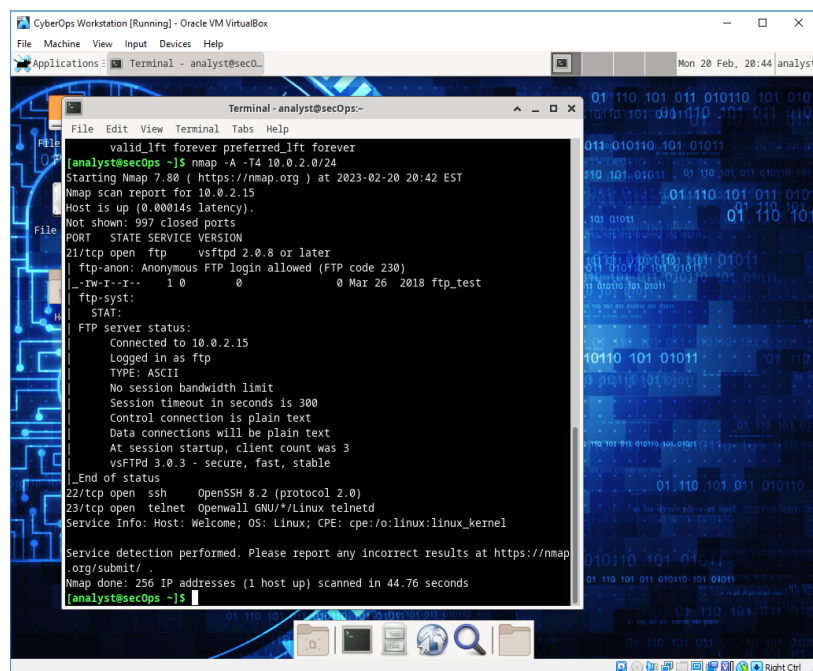
3. Network Scanning

Sebelum melakukan scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu dengan perintah **ip address**



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
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 ~]$ ip host  
Object "host" is unknown, try "ip 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 82297sec preferred_lft 82297sec  
    inet6 fe80::a00:27ff:fe06:b93a/64 scope link  
        valid_lft forever preferred_lft forever  
[analyst@secOps ~]$
```

Lakukan port scanning dengan menggunakan Nmap perintahnya **nmap -A -T4 10.0.2.0/24**



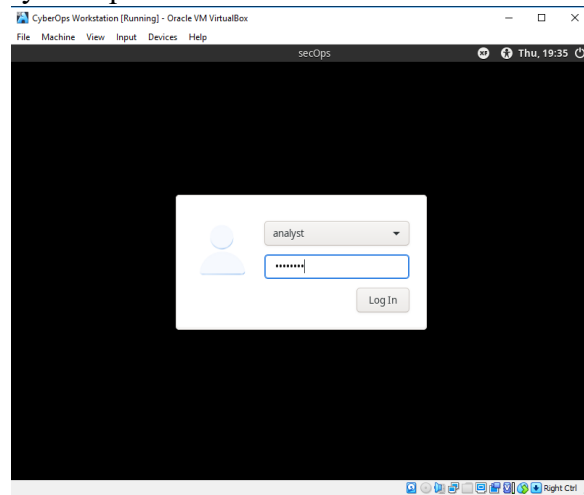
```
CyberOps Workstation [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Applications: Terminal - analyst@secOps... Mon 20 Feb, 20:44 analyst  
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
valid_lft forever preferred_lft forever  
[analyst@secOps ~]$ nmap -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  
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 ~]$
```

Unit 3 Pemantauan Trafik

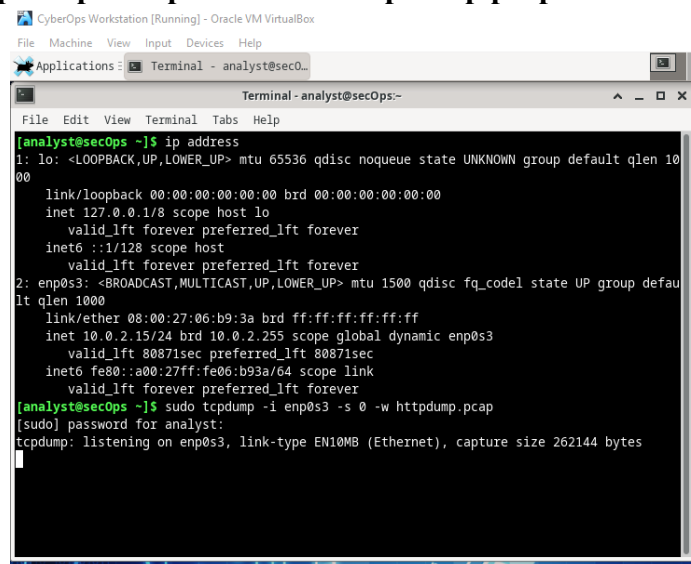
1. Jalankan VM CyberOps Workstation dan Login

Username : analyst

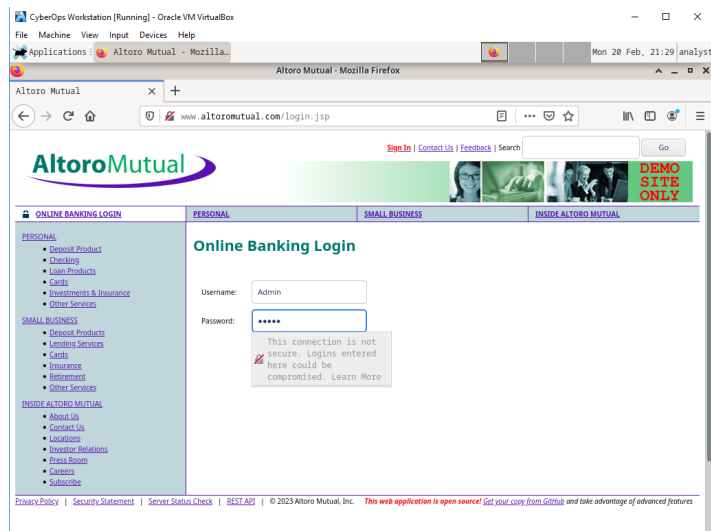
Password : cybercops



2. Buka terminal dan menjalankan tcpdump
Pengecekan alamat IP dengan menggunakan perintah:
ip address
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap

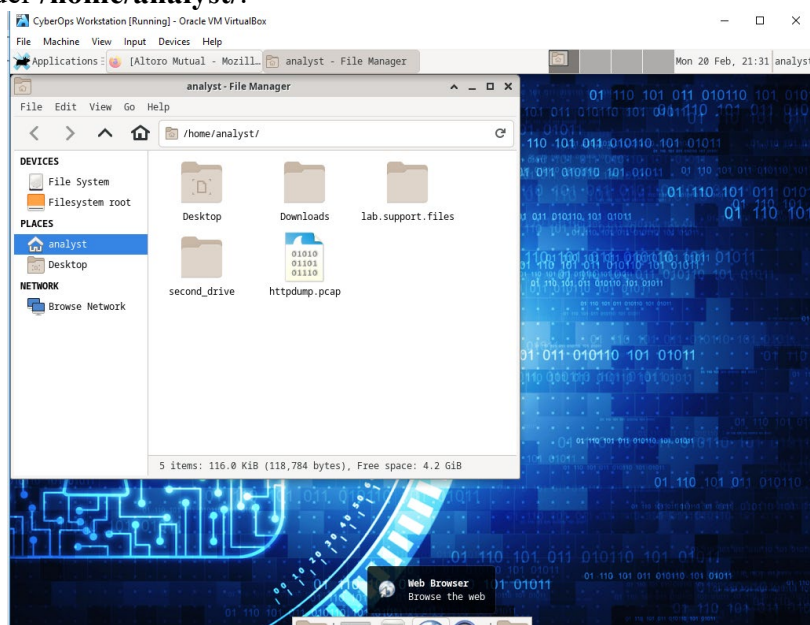


3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM.
Username : **Admin**
Password : **Admin**

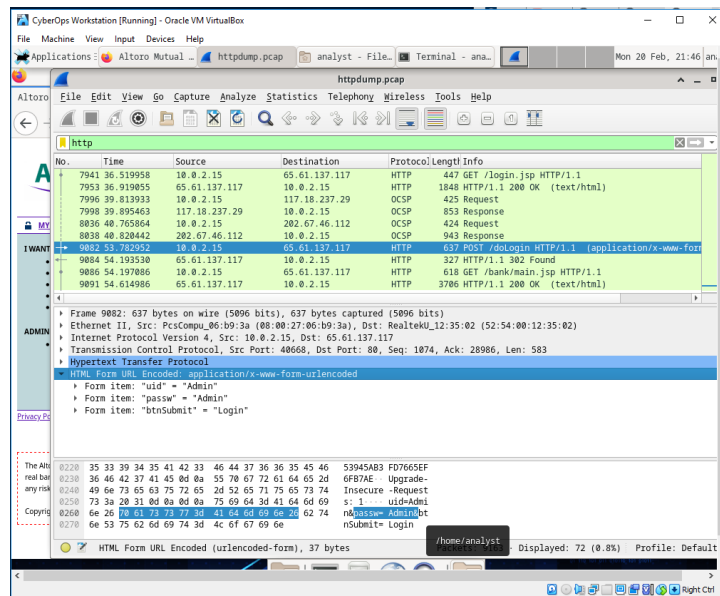


4. Merekam Paket HTTP

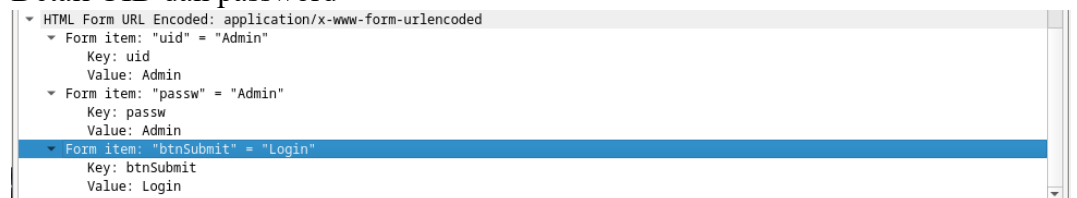
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder `/home/analyst/`.



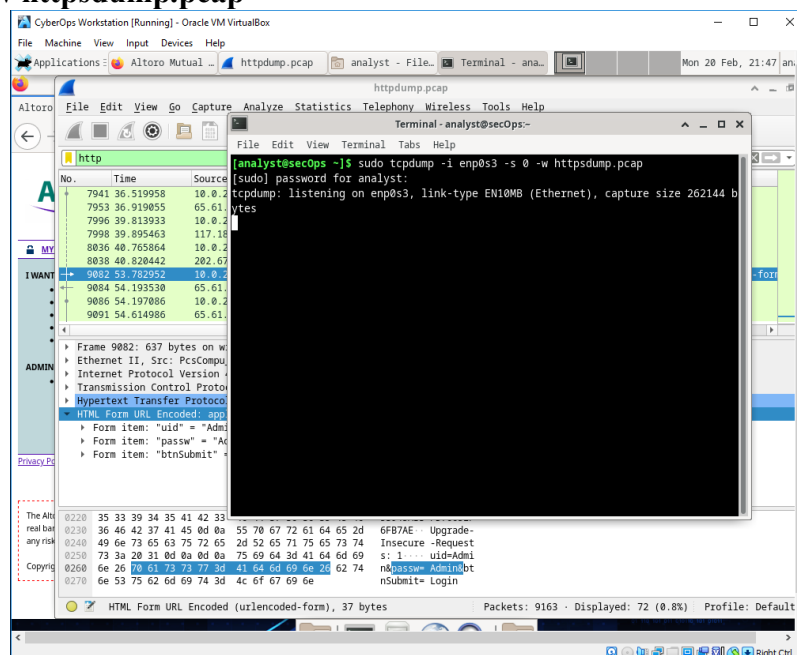
5. Filter http kemudian klik Apply pilih POST



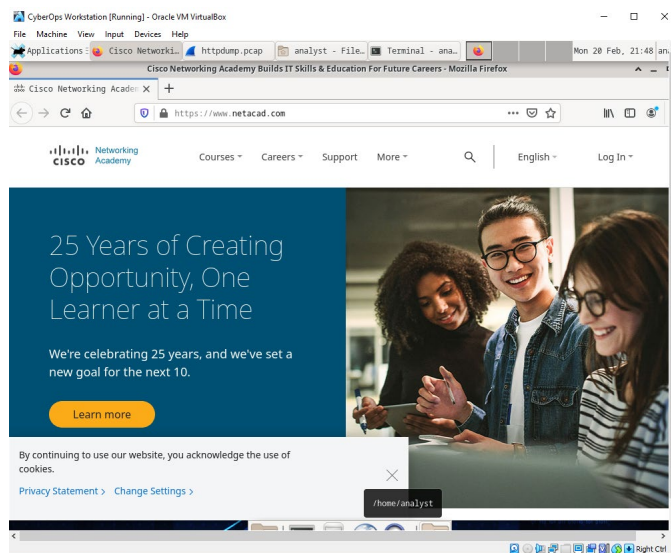
6. Detail UID dan password



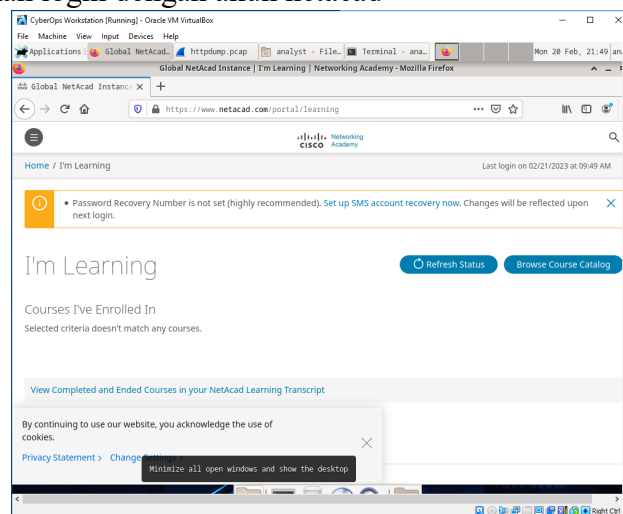
7. Merekam paket HTTPS dengan perintah `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`



8. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM.



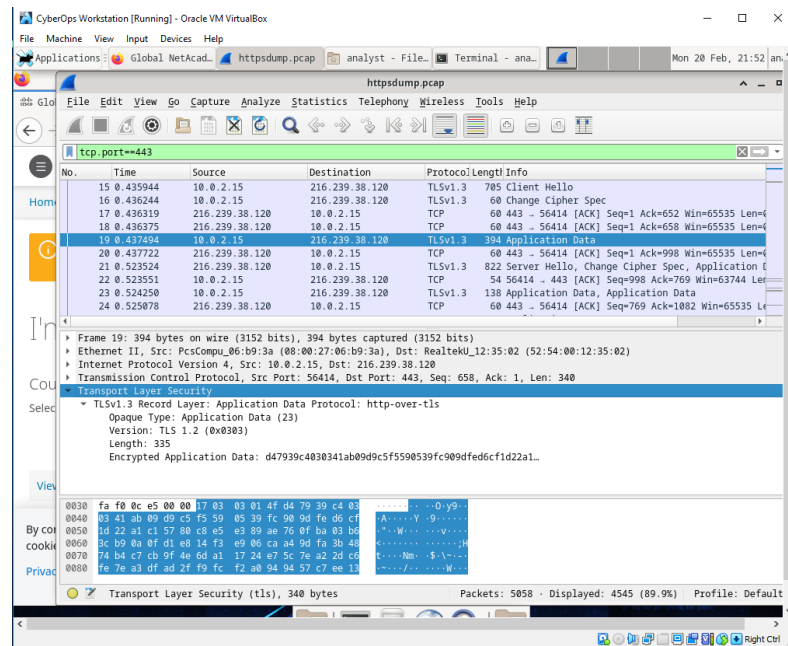
9. Lalu lakukan login dengan akun netacad



10. Melihat rekaman paket HTTPS

Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder `/home/analyst/`

11. Filter `tcp.port==443` lalu pilih **Application Data**



C. PEMBAHASAN

Unit 2

1. Eksplorasi NMAP

Nmap ("Network Mapper") adalah alat sumber terbuka untuk eksplorasi jaringan dan audit keamanan. Itu dirancang untuk memindai jaringan besar dengan cepat, meskipun bekerja dengan baik terhadap host tunggal. Nmap menggunakan paket IP mentah dengan cara baru untuk menentukan host apa yang tersedia di jaringan, layanan apa (nama dan versi aplikasi) yang ditawarkan host tersebut, sistem operasi (dan versi OS) apa yang mereka jalankan, jenis filter paket/firewall apa sedang digunakan, dan lusinan karakteristik lainnya. sementara Nmap umumnya digunakan untuk audit keamanan, banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas-tugas rutin seperti inventaris jaringan, jadwal peningkatan layanan nanaging, dan pemantauan host atau uptime layanan.

Keluaran dari Nmap adalah daftar target yang dipindai, dengan informasi tambahan adalah tabel port yang menarik ". informasi masing-masing tergantung pada opsi yang digunakan. Kunci di antaranya Tabel tersebut mencantumkan nomor port dan protokol, nane layanan, dan status. Status apakah open, filtered, closed, atau unfiltered Open artinya sebuah aplikasi pada nachine target mendengarkan koneksi/paket pada itu Filtered artinya firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga inap tidak dapat mengetahui apakah itu terbuka atau tertutup. Port tertutup tidak

memiliki aplikasi yang mendengarkan pada saat itu, meskipun mereka dapat terbuka kapan saja. Port diklasifikasikan sebagai tidak tersaring ketika responsif terhadap probe tidur siang, tetapi tidur siang tidak dapat menentukan apakah terbuka atau tertutup. laporan tidur siang kombinasi status open filtered dan closed filtered ketika tidak dapat menentukan termasuk perangkat lunak yang mana dari dua status yang menjelaskan port.

NMAP merupakan salah satu aplikasi yang memiliki keunggulan dan peran terutama dalam keamanan jaringan. Adapun fungsi dari NMAP di antaranya:

a. Digunakan untuk memeriksa jaringan

Fungsi utama NMAP adalah mengecek dan memeriksa sebuah jaringan. Pengecekan oleh NMAP dapat dilakukan sekalipun pada jaringan yang besar dan kurun waktu yang singkat. NMAP dapat bekerja pada host tunggal dengan cara menggunakan IP raw sebagai penentu nama dari host yang disediakan pada suatu jaringan.

IP raw ini dapat berfungsi untuk melihat dan mengetahui layanan apa saja yang tersedia dengan nama dan versi aplikasi di dalamnya, sistem operasi lengkap dengan versinya, serta jenis-jenis firewall dan paket filter apa saja yang digunakan.

Penggunaan NMAP memudahkan para penggunanya dalam mendapatkan informasi secara lengkap mengenai jaringan maupun host itu sendiri.

b. Melakukan scanning atau pemindaian pada port jaringan

NMAP selanjutnya adalah melakukan pemindaian pada port yang ada di dalam sebuah jaringan komputer. Port itu sendiri merupakan nomor yang digunakan dalam membedakan aplikasi satu dengan yang lainnya yang ada dalam satu jaringan komputer.

Dengan adanya NMAP, kita dapat melakukan pemindaian atau scanning pada masing-masing port serta dapat mengetahui aplikasi apa saja yang sudah terpasang pada suatu perangkat.

c. Sebagai Discover Vulnerabilities dan Version Detection

Discover vulnerabilities yang dimaksudkan di sini adalah NMAP berperan dalam menemukan kerentanan yang dapat terjadi di dalam sebuah jaringan.

Sedangkan version detection yang dimaksud adalah untuk mengecek dan memeriksa setiap layanan jaringan yang terdapat di dalam perangkat jarak jauh. Serta menentukan nama aplikasi apa yang dipasang lengkap dengan versinya.

2. Localhost Scanning

Setelah melakukan *Localhost Scanning* dengan perintah **nmap -A -T4 localhost** dapat diketahui port yang terbuka adalah

Port terbuka	Layanan	Software yang digunakan
21	ftp	vsftpd
22	ssh	OpenSSH
23	telnet	Openwall GNU

Hal ini dapat dilihat pada output perintah yang diberikan seperti pada gambar di bawah ini:

```
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
```

3. Network Scanning

- a. Setelah memasukkan perintah **ip address** dapat diketahui alamat ip host-nya adalah 10.0.2.15 dan subnetmask dari PC host adalah 255.255.255.0 hal ini diketahui dari output perintah yang dimasukkan:

```
[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
```

- b. Setelah mengetahui alamat IP dan subnetmask dari PC host selanjutnya adalah melakukan port scanning dengan menggunakan nmap. Hal ini bertujuan untuk mengetahui port layanan yang terbuka dan juga mengetahui jumlah host yang terdeteksi menggunakan jaringan tersebut. Untuk melakukan port scanning ini dapat dengan perintah **nmap -A -T4 (ip network)** dan keluarannya adalah terdapat 1 host yang terdeteksi terlihat pada bagian seperti pada gambar di bawah ini:

```
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 ~]$
```

Unit 3

HTTP (Hypertext Transfer Protocol)

HTTP adalah sebuah protocol jaringan lapisan aplikasi yang digunakan untuk membantu proses pertukaran data dalam internet antar computer saty dengan lainnya. Protokol ini menggunakan hipermedia yang dihubungkan dengan link disebut dokumen hypertext yang membentuk WWW atau World Wide Web.

HTTP adalah protokol yang menyediakan perintah dalam komunikasi antar jaringan, di mana hal ini yaitu komputer client dengan web server. Nantinya, komputer client akan melakukan request dengan mengakses domain URL maupun alamat IP. Kemudian request tersebut akan dikelola atau dijalankan oleh web server sesuai kode yang dimasukkan.

Protokol HTTP didesain untuk mengelola dokumen HTML dan mengirimkannya kepada client, itulah sebabnya protokol berikut paling banyak digunakan dibanding dengan protocol lain.

Keunggulan HTTP

1. Mendukung implementasi dengan protokol lain di internet dan jaringan lainnya.
2. Halaman HTTP disimpan di komputer dan cache, sehingga lebih cepat diakses.
3. Tidak bergantung pada platform tertentu dan memungkinkan porting lintas platform.
4. Tidak memerlukan dukungan runtime apapun.
5. Dapat digunakan melalui firewall.
6. Tidak berorientasi koneksi, sehingga tidak ada overhead jaringan untuk memelihara status dan informasi sesi.

Kekurangan HTTP

1. Tidak ada privasi karena siapa saja bisa melihat konten.
2. Integritas data tidak terjamin karena siapapun bisa mengubah konten.
3. Hacker yang berhasil mengintersepsi data Anda dapat membaca informasi apapun yang terdapat di dalamnya

HTTPS

HTTPS adalah hasil penyempurnaan HTTP yang dilakukan oleh Netscape Communications pada tahun 1994. Tujuan awal pengembangan HTTPS adalah untuk digunakan di Netscape Navigator, produk web browser milik Netscape.

Hal yang paling membedakan HTTP dan HTTPS adalah dari segi keamanan. HTTP masih mengirimkan data dalam format plain text (teks biasa), sedangkan HTTPS sudah menggunakan enkripsi.

Sederhananya, data yang dikirimkan lewat HTTPS 'dikunci' terlebih dahulu agar tidak dicuri oleh orang lain. Sekalipun ada orang yang berusaha mencurinya, orang tersebut tidak akan bisa membaca isinya karena tidak memiliki 'kunci'. Mekanisme ini disebut dengan enkripsi.

Keunggulan HTTPS

1. Pada kebanyakan kasus, situs yang menggunakan HTTPS akan memiliki redirect. Sekalipun pengguna mengetikkan `http://`, pengguna tetap akan dialihkan ke `https://`.
2. Memungkinkan pengguna untuk bertransaksi secara aman, contohnya seperti dompet digital, trading, dan online banking.
3. Teknologi SSL melindungi pengguna dan membangun kepercayaan.
4. Otoritas independen memverifikasi identitas pemilik sertifikat. Setiap sertifikat SSL berisi informasi terautentikasi tentang pemiliknya.

Kekurangan HTTPS

1. Protokol HTTPS tidak bisa melindungi data yang tersimpan di browser sebagai cache.
2. Data hanya dienkripsi selama transmisi tanpa bisa menghapus teks dari memori browser.
3. Dapat menimbulkan overhead jaringan dan komputasi.

Perbedaan HTTP dan HTTPS

Perbedaan yang paling menonjol diantara HTTP dan HTTPS adalah pada HTTPS sudah menggunakan enkripsi. Dengan adanya enkripsi ini, website akan jadi lebih sulit untuk ditembus hacker karena pertukaran data di dalamnya sudah dilindungi. Berikut adalah beberapa perbedaan HTTP dan HTTPS lainnya:

1. Penggunaan Port
HTTP menggunakan port 80, dimana komunikasi data masih menggunakan teks biasa, sehingga rentan diretas. Sedangkan, port HTTPS adalah port 443 yang lebih aman di mana setiap komunikasi atau transfer data terenkripsi, sehingga tidak mudah dibaca pihak lain.
2. Penggunaan SSL

SSL adalah metode akses website menggunakan sambungan protokol terenkripsi. HTTP adalah protokol yang belum memanfaatkan sertifikat keamanan SSL. Sedangkan, HTTPS sudah menggunakan SSL/TLS (Transport Layer Secure) untuk enkripsi data.

Dengan SSL aktif pada HTTPS, ketika browser meminta data dari web server, pesan akan diacak. Dengan begitu, hanya dapat terbaca dengan baik oleh website yang memiliki kunci enkripsi yang ditentukan.

3. Keamanan Data

HTTPS menggunakan tiga prosedur keamanan data yaitu autentikasi server, enkripsi data, dan integritas data. Hal ini tidak ditemukan pada protokol HTTP. Autentikasi server dapat memastikan pengguna melakukan komunikasi dengan situs yang benar. Sehingga, HTTPS dapat menghindari serangan man-in-the-middle atau penyusup saat pertukaran data terjadi. Selanjutnya, enkripsi data dilakukan untuk menjaga dari pencurian dan penyadapan selama transfer data sedang berlangsung.

Wireshark

Melihat Segment TCP yang ada dalam jaringan bisa dilakukan dengan menggunakan program aplikasi, salah satu contohnya adalah wireshark. Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Seperti namanya, Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:

- Troubleshooting masalah di jaringan
- Memeriksa keamanan jaringan
- Sniffer data-data privasi di jaringan

Wireshark adalah salah satu program untuk menganalisis suatu jaringan, baik itu jaringan kabel maupun jaringan nirkabel. Perangkat ini digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan.

Wireshark adalah mungkin salah satu analisa terbaik paket open source yang tersedia saat ini. Beberapa tujuan penggunaan wireshark

- administrator jaringan menggunakannya untuk memecahkan masalah jaringan
- insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan
- pengembang menggunakannya untuk men-debug implementasi protokol
- beberapa orang menggunakannya untuk mempelajari protokol jaringan internal

Analisa terhadap pemantauan traffic HTTP dan HTTPS

Pada saat melakukan pemantauan traffic pada HTTP yang dipantau adalah pada bagian POST yang mana POST digunakan untuk mengirim data yang biasanya di gunakan untuk menambah/merubah data pada server. Pada praktikum kali ini dilakukan memasukkan User ID dan passwordnya yang mana dengan memasukkan ini akan menambah data pada server. Karena server menggunakan protocol HTTP dengan port 80 yang mana masih menggunakan teks biasa sehingga ketika dipantau menggunakan wireshark UID dan password masih dapat dilihat.

Pada saat melihat rekaman paket HTTPS yang didapat adalah pada data aplikasi terenkripsi sehingga ketika dipantau tidak terdapat data apapun. HTTPS sudah menggunakan SSL/TLS (Transport Layer Secure) untuk enkripsi data. Dengan SSL aktif pada HTTPS, ketika browser meminta data dari web server, pesan akan diacak. Dengan begitu, hanya dapat terbaca dengan baik oleh website yang memiliki kunci enkripsi yang ditentukan.

D. KESIMPULAN

Adapun kesimpulan yang dapat diambil dari dilaksanakan praktikum kali ini adalah:

- HTTP merupakan protocol jaringan lapisan aplikasi yang digunakan untuk membantu proses pertukaran data dalam internet dan komunikasi data masih menggunakan teks sehingga rentan diretas.
- HTTPS merupakan penyempurnaan HTTP dimana dalam pertukaran datanya dienkripsi sehingga data tidak mudah dibaca oleh pihak lain.

E. DAFTAR PUSTAKA

Penulis. (2022, October 12). *Mengenal Perbedaan HTTP Dan HTTPS*.

IDwebhost. <https://idwebhost.com/blog/http-dan-https/>

Wijayanti, N. N. (2023, January 4). *Perbedaan HTTP Dan HTTPS: Ini Penyebab*

HTTPS Lebih Aman! Niagahoster Blog.

<https://www.niagahoster.co.id/blog/perbedaan-http-dan-https/>