TUGAS
KEAMANAN SISTEM INFORMASI
2.4.7 Lab Video - Use Wireshark to Compare Telnet and SSH Traffic

Anisatul Latifah
2141762008
SIB – 4C

POLITEKNIK NEGERI MALANG
2024/2025

Lab - Use Wireshark to Compare Telnet and SSH Traffic

Tujuan

- Gunakan Wireshark untuk menangkap lalu lintas peramban web.
- Gunakan Wireshark untuk menangkap lalu lintas Telnet.
- Gunakan Wireshark untuk menangkap lalu lintas SSH.

Latar Belakang / Skenario

Wireshark adalah penganalisis protokol jaringan yang memungkinkan Anda melihat apa yang terjadi di jaringan Anda pada tingkat mikroskopis. Anda dapat menangkap paket dan menyimpannya untuk analisis offline. Wireshark menyertakan banyak alat untuk pemeriksaan mendalam terhadap ratusan protokol jaringan. Di lab ini, Anda akan menggunakan Wireshark untuk menangkap dan memeriksa lalu lintas web, lalu lintas Telnet, dan lalu lintas SSH.

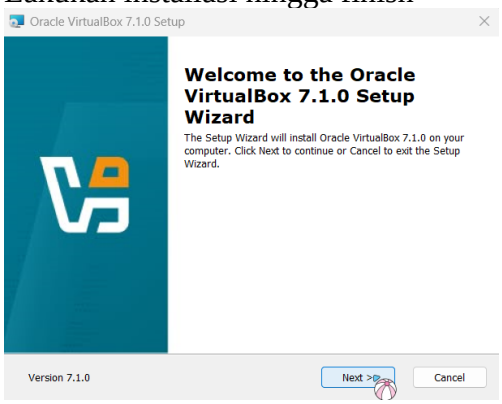
Sumber Daya yang Diperlukan

PC dengan **CSE-LABVM** terinstal di VirtualBox

INSTALLASI VIRTUAL BOX

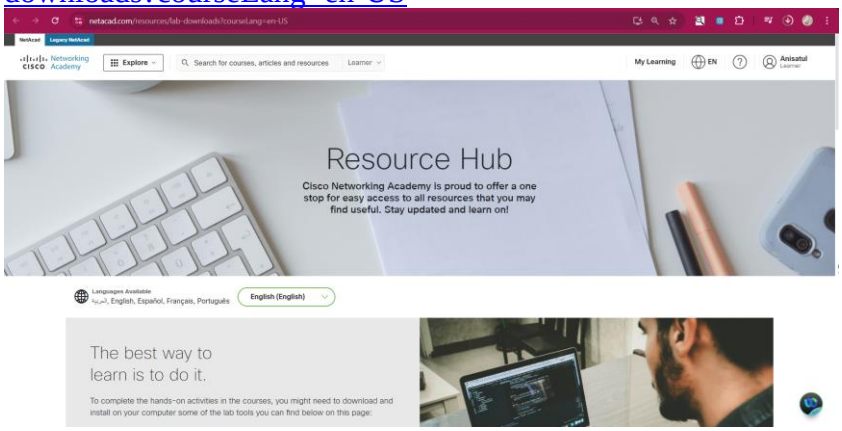
1. Download virtual box terlebih dahulu

2. Lakukan installasi hingga finish

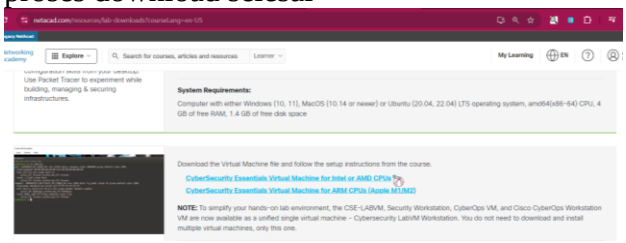


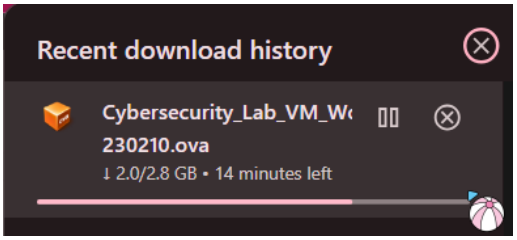
INSTALLASI CSE-LABVM

1. Download CSE-LABVM pada link https://www.netacad.com/resources/lab-downloads?courseLang=en-US

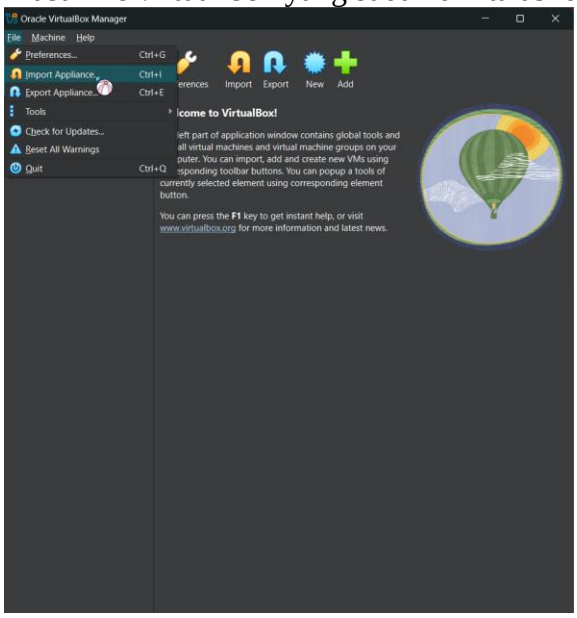


2. Pilih CyberSecurity Essentials Virtual Machine for Intel or AMD CPUs dan tunggu hingga proses download selesai

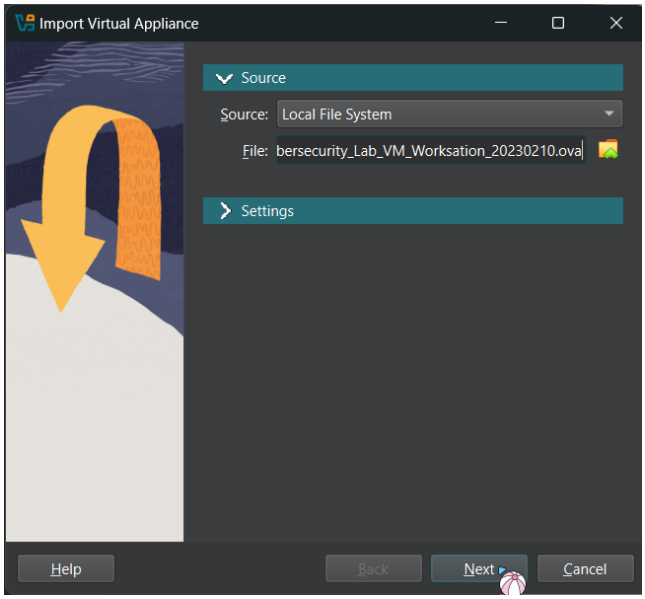




3. Masuk ke virtual box yang sudah diintalasi dan pilih File > Import Appliance

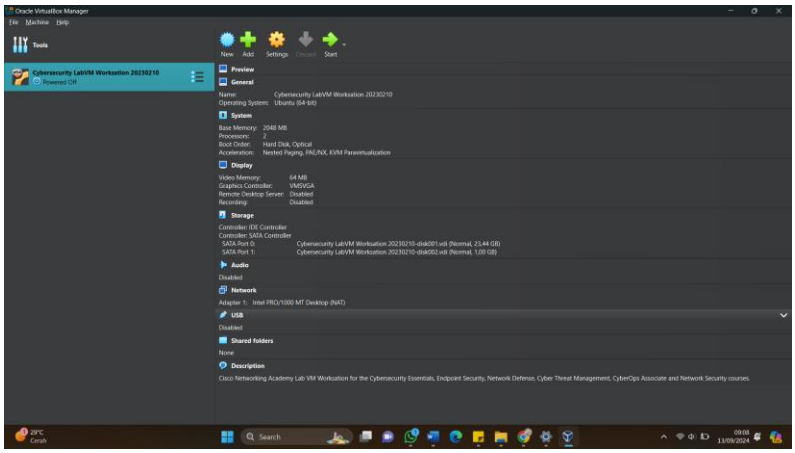


4. Xx

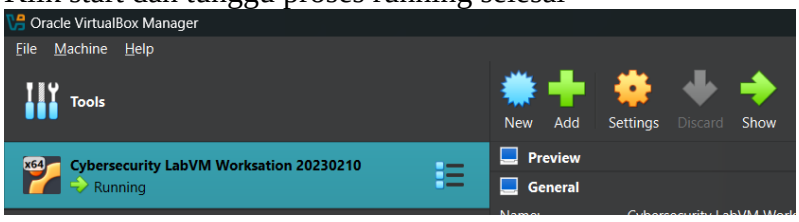


5. Tunggu sampai selesai

6. LabVm sudah terinstall



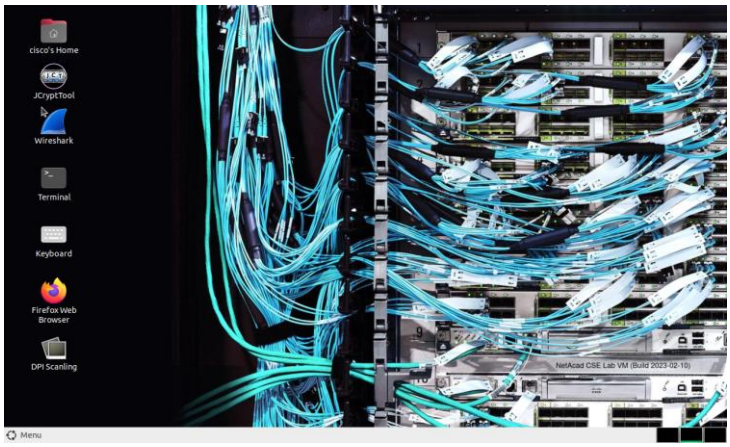
7. Klik start dan tunggu proses running selesai



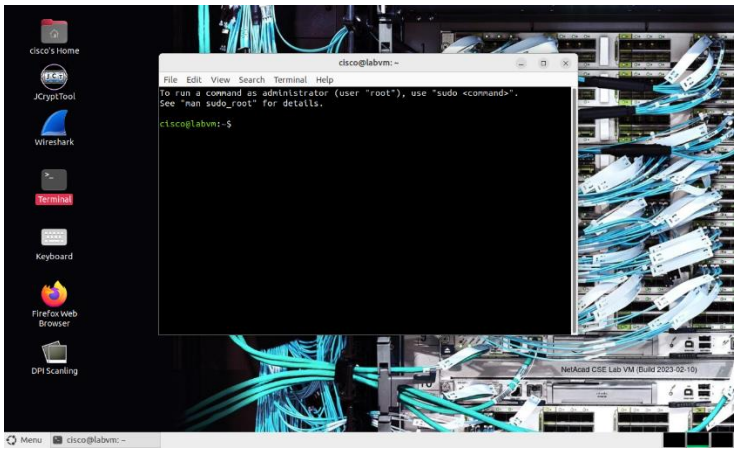
Instruksi

Langkah 1: Buka jendela terminal di CSE-LABVM.

a. Luncurkan **CSE-LABVM** .



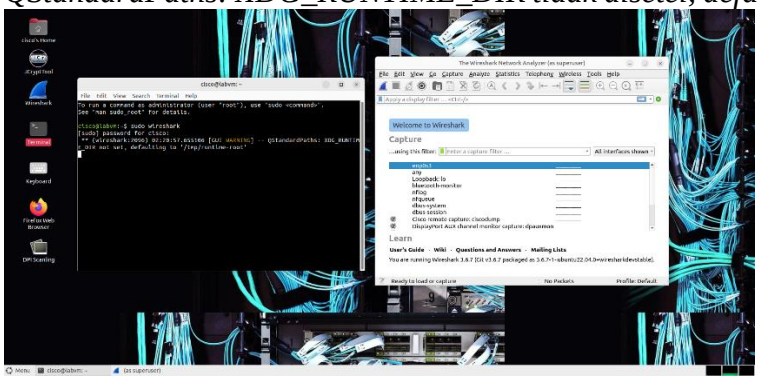
b. Klik dua kali ikon **Terminal** untuk membuka terminal.



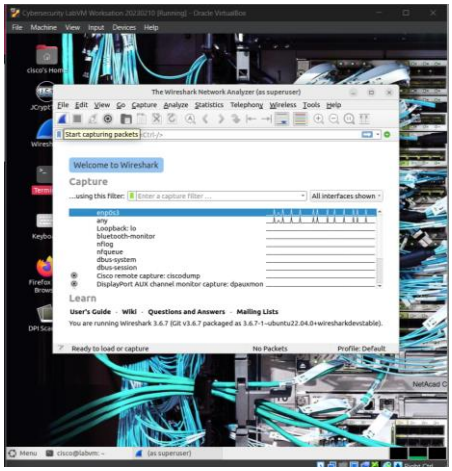
Langkah 2: Jelajahi penganalisis protokol Wireshark.

a. Untuk menangkap lalu lintas pada VM Anda, Anda perlu menjalankan Wireshark dalam mode promiscuous, yang mengharuskan menjalankan dengan hak istimewa yang ditingkatkan menggunakan **sudo** . Masukkan perintah **sudo wireshark** , lalu masukkan **kata sandi** untuk kata sandi. Antarmuka pengguna grafis (GUI) Wireshark akan terbuka.

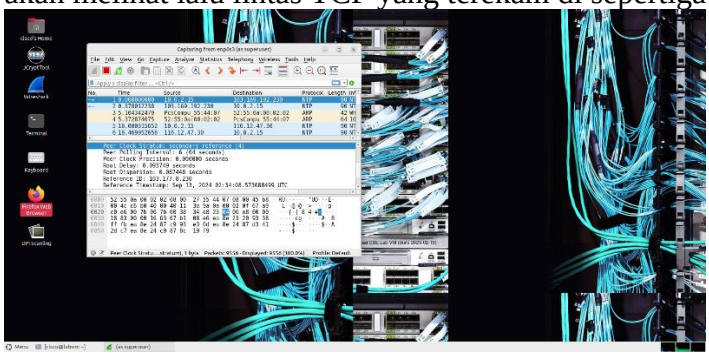
cisco@labvm:~$ ***sudo wireshark***
[sudo] kata sandi untuk cisco: ***kata sandi***
QStandardPaths: XDG_RUNTIME_DIR tidak disetel, defaultnya adalah '/tmp/runtime-root'



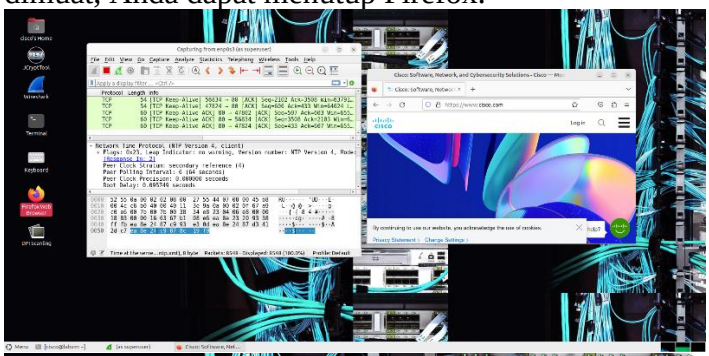
b. Di bawah daftar antarmuka, pilih **salah satu** , lalu klik **Capture** > **Start** dari menu. Atau, Anda dapat mengklik ikon sirip hiu. Wireshark akan mulai menangkap paket.

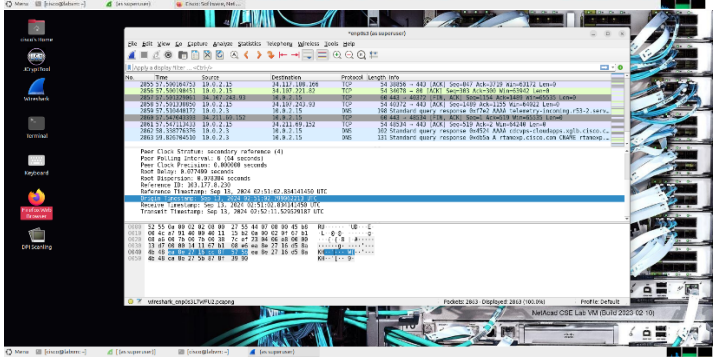


c. Jika Firefox sudah terbuka, Anda mungkin melihat lalu lintas yang terekam di antarmuka Wireshark. Jika Firefox belum terbuka, silakan buka sekarang. Di Wireshark, Anda sekarang akan melihat lalu lintas TCP yang terekam di sepertiga bagian atas jendela.

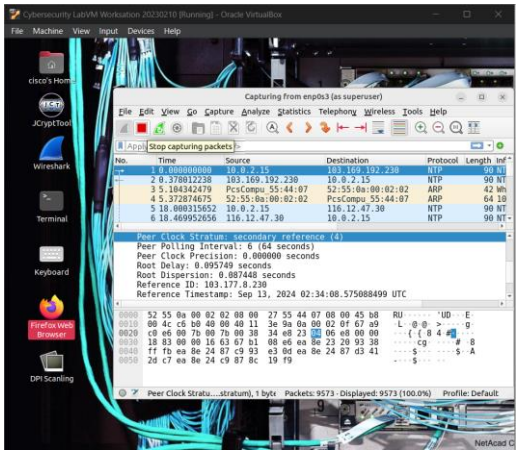


d. Di Firefox, masukkan www.cisco.com untuk mengunjungi situs web Cisco. Setelah situs web dimuat, Anda dapat menutup Firefox.





e. Kembali ke Wireshark dan klik **Capture** > **Stop** dari menu. Atau, Anda dapat mengklik tombol kotak merah di samping sirip hiu.

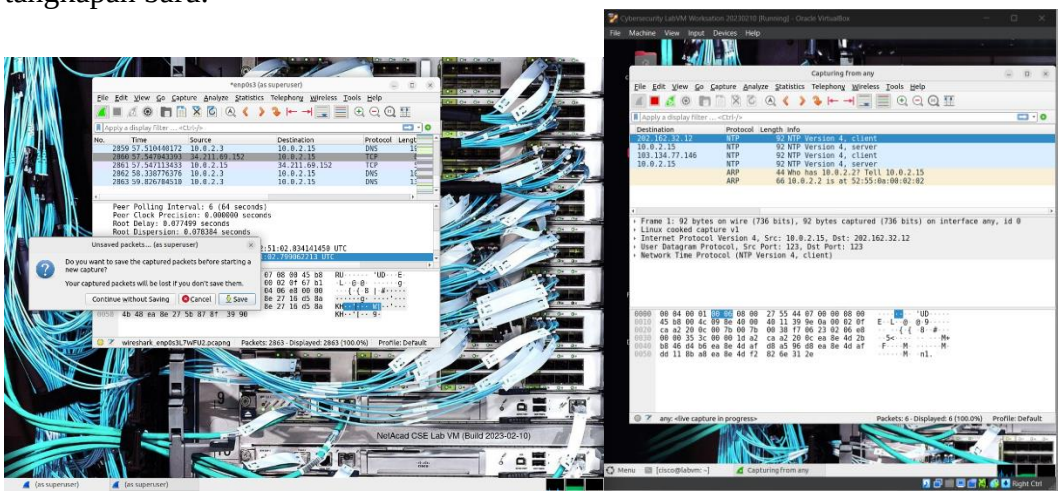


f. Di Wireshark, Anda akan melihat bidang filter dan tiga panel kunci atau area kerja:

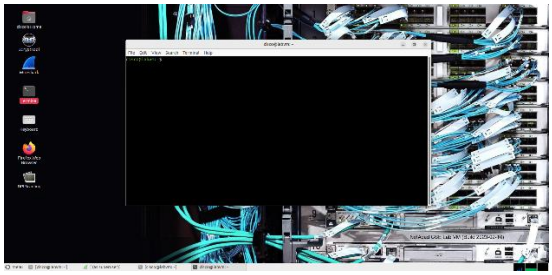
- Bidang **Terapkan filter tampilan** berada tepat di bawah bilah alat.
- **Daftar Paket** mencakup kolom-kolom berikut untuk setiap paket yang ditangkap:
  - **Tidak** - nomor paket (dalam urutan numerik).
  - **Waktu** - stempel waktu paket
  - **Sumber** - alamat IP sumber paket
  - **Tujuan** - alamat IP tujuan paket
  - **Protokol** - protokol paket
  - **Panjang** - jumlah byte yang ditangkap untuk paket ini
  - **Info** - informasi tambahan tentang isi paket
- Panel **Rincian Paket** menampilkan protokol dan kolom protokol dari paket yang dipilih. Perhatikan bahwa kolom tersebut dapat diperluas atau diciutkan dengan mengeklik tanda panah di samping kolom tersebut.
- Panel Packet **Bytes** menampilkan detail byte dari paket yang dipilih. Saat Anda memilih bagian paket di panel Packet Details, byte yang sesuai akan disorot di panel Packet Bytes. Sisi kiri menampilkan representasi heksadesimal dari byte, dan sisi kanan menampilkan representasi ASCII.

Langkah 3: Menangkap dan menganalisis lalu lintas Telnet yang tidak terenkripsi.

a. Mulai tangkapan baru. Di kotak dialog **Paket yang belum disimpan… , klik Lanjutkan tanpa Menyimpan** . Ini akan menghapus paket dari tangkapan terakhir Anda dan memulai tangkapan baru.

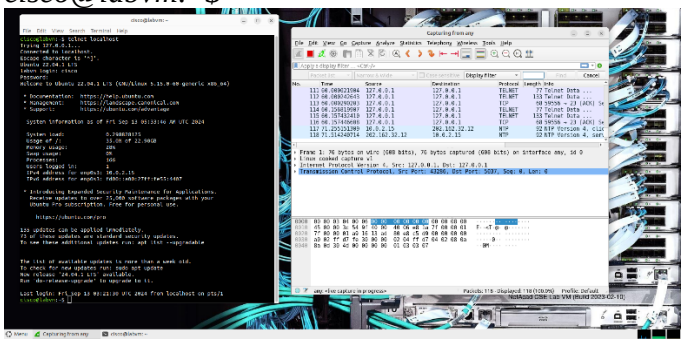


b. Klik dua kali ikon **Terminal** untuk membuka jendela terminal baru.



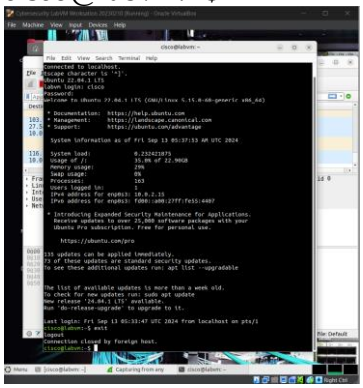
c. Anda dapat melakukan simulasi login jarak jauh ke VM Anda dengan memasukkan perintah **telnet localhost** , lalu login sebagai **cisco** dengan **kata sandi** sebagai kata sandinya.

cisco@labvm:~$ ***telnet localhost***
Mencoba ::1...
Mencoba 127.0.0.1...
Terhubung ke localhost.
Karakter escape adalah '^]'.
Ubuntu 20.04.2 LTS
labvm masuk: ***cisco***
Kata sandi: ***kata sandi***
Selamat datang di Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)
** Dokumentasi: https://help.ubuntu.com*
** Manajemen: https://landscape.canonical.com*
** Dukungan: https://ubuntu.com/advantage*
0 pembaruan dapat segera diinstal.
0 dari pembaruan ini adalah pembaruan keamanan.
Login terakhir: Kamis 18 Mar 21:47:23 UTC 2021 pada tty2
cisco@labvm:~$

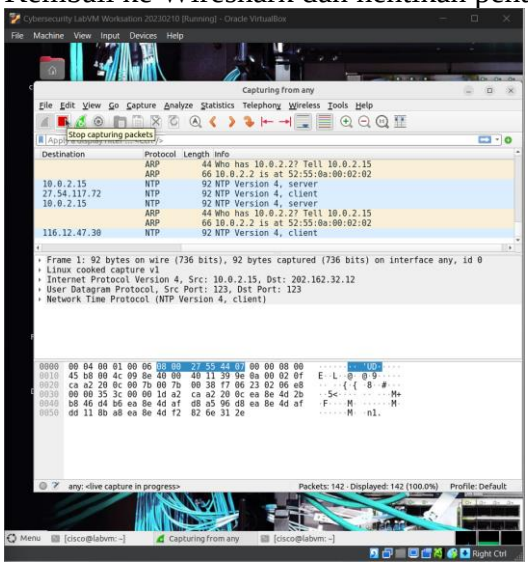


d. Masukkan perintah **exit** untuk mengakhiri sesi Telnet:

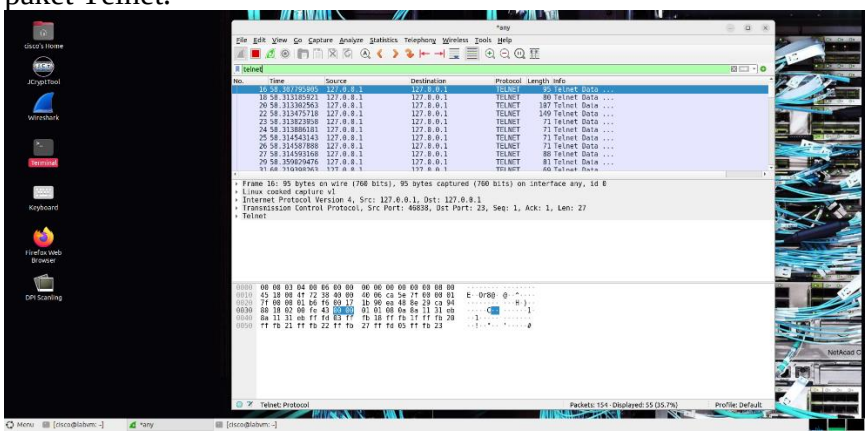
cisco@labvm:~$ ***keluar***
keluar
Koneksi ditutup oleh host asing.
cisco@labvm:~$



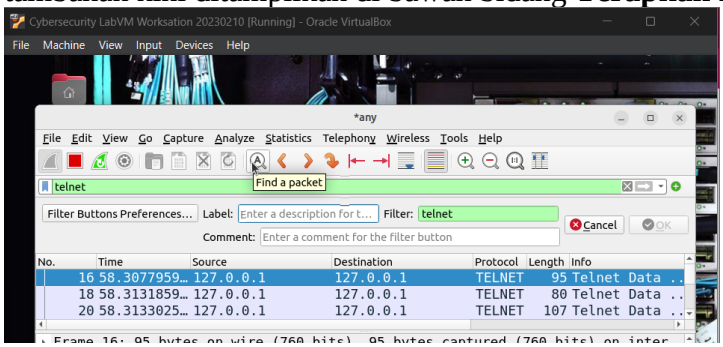
e. Kembali ke Wireshark dan hentikan penangkapan.



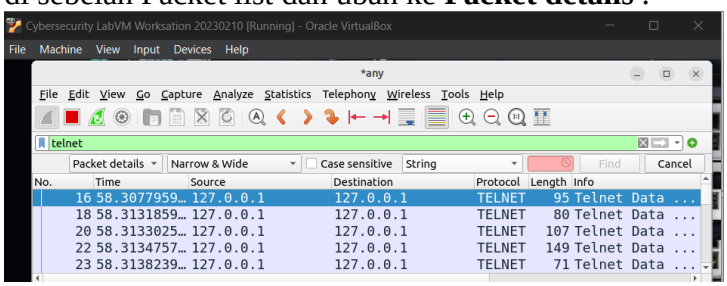
f. Pada kolom **Terapkan filter tampilan** , ketik **telnet** lalu tekan **Enter** untuk memfilter hanya paket Telnet.



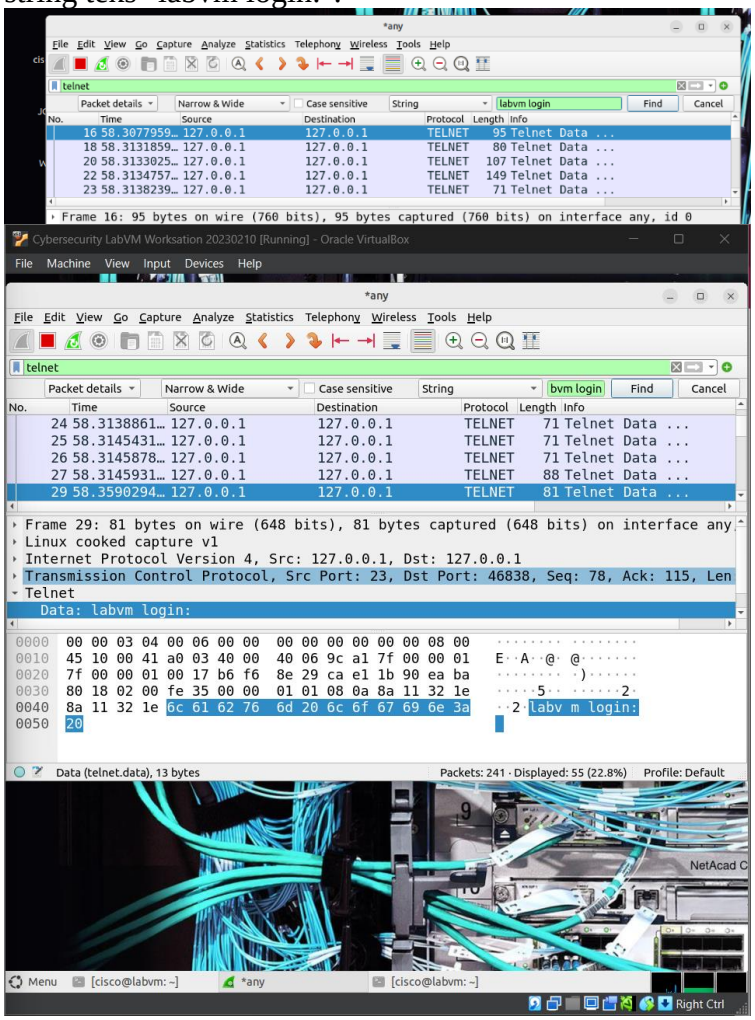
g. Pada bilah alat, klik ikon kaca pembesar untuk **Menemukan paket** . Fitur pencarian tambahan kini ditampilkan di bawah bidang **Terapkan filter tampilan** .



h. Klik tanda panah di sebelah **Display filter** dan ubah ke **String** . Kemudian klik tanda panah di sebelah Packet list dan ubah ke **Packet details** .



i. Untuk menemukan paket yang meminta informasi login, ketik **labvm login:** di kolom di sebelah **String** , lalu tekan **Enter** atau klik **Find** . Wireshark akan menyorot paket yang berisi string teks "labvm login:".



j. Di panel **Rincian Paket** , klik tanda panah di samping **Telnet** untuk memperluas isinya. Anda akan melihat bahwa **labvm login:** adalah data untuk paket ini. Data untuk paket tersebut juga ditampilkan di panel **Byte Paket** . Anda dapat mengetahui bahwa teks tersebut dikirim tanpa enkripsi karena Anda dapat membacanya.

k. Di panel **Daftar Paket** , klik paket yang disorot dengan **labvm login** sebagai data untuk memilihnya.

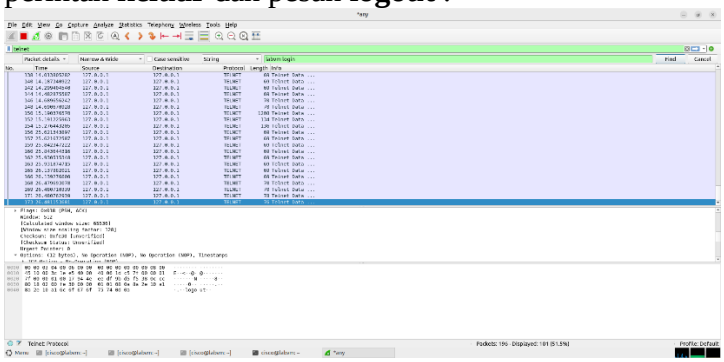
l. Untuk menemukan nama pengguna dan kata sandi, gunakan panah bawah pada papan ketik untuk memilih paket berikutnya. Di panel **Rincian Paket** , Anda akan melihat nilai untuk **Data** di bawah **Telnet** adalah huruf pertama yang Anda ketik di bidang untuk perintah "labvm login:", yang merupakan **c** untuk **cisco** . Jika Anda mengklik panah bawah lagi, Anda akan melihat data paket berikutnya juga **c** . Ini karena paket tersebut dicantumkan dua kali: satu kali untuk sumber yang mengirim ke tujuan dan sekali lagi untuk tujuan yang menerima paket. Karena sumber dan tujuan adalah antarmuka yang sama (loopback 127.0.0.1), paket tersebut dicantumkan dua kali oleh Wireshark.

m. Terus tekan tombol panah bawah hingga Anda mencapai paket terakhir dengan nilai data **o** untuk nama pengguna **cisco** .

n. Terus klik tanda panah bawah hingga Anda melihat **Kata Sandi:** di bidang **Data** . Terus tekan tanda panah bawah untuk membaca data dari delapan paket berikutnya yang akan mengungkapkan, satu huruf pada satu waktu, bahwa **kata sandi** adalah kata sandi untuk pengguna **cisco** .

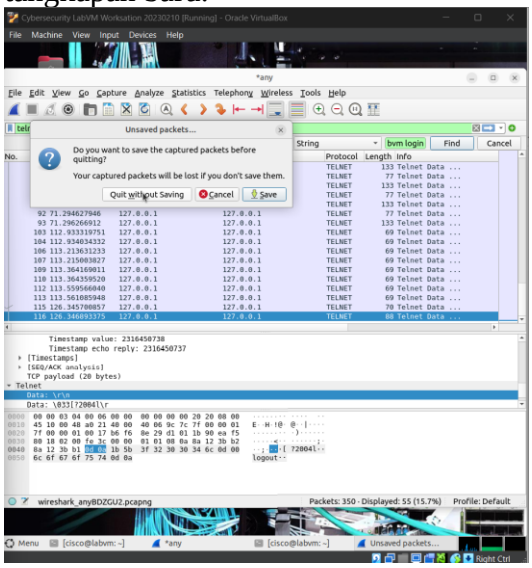
Screen Recorder j-n :
https://bit.ly/ScreenRecorderJ-N

o. Jika Anda terus menekan tombol panah bawah pada sisa paket yang ditangkap, Anda akan melihat semua teks yang dikirim dan diterima selama sesi Telnet, termasuk perintah **keluar** dan pesan **logout** .

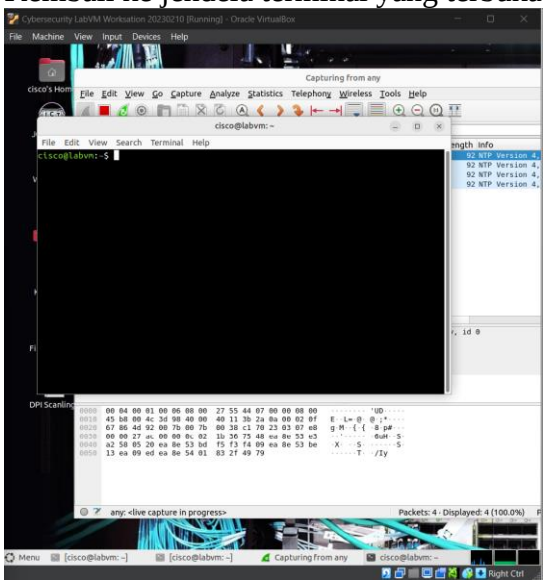


Langkah 4: Menangkap dan menganalisis lalu lintas SSH yang terenkripsi.

a. Mulai tangkapan baru. Di kotak dialog **Paket yang belum disimpan… , klik Lanjutkan tanpa Menyimpan** . Ini akan menghapus paket dari tangkapan terakhir Anda dan memulai tangkapan baru.

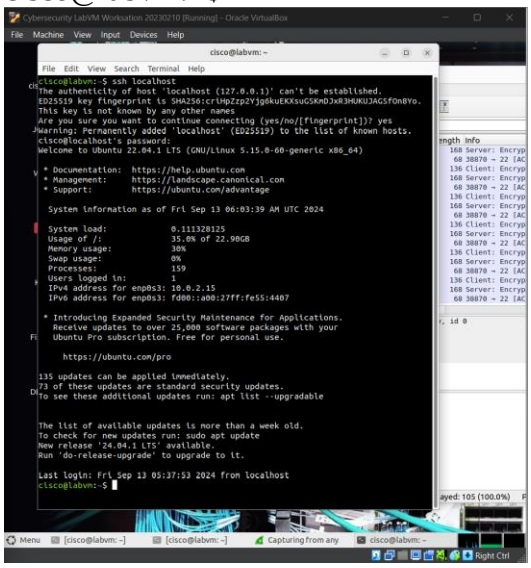


b. Kembali ke jendela terminal yang terbuka atau mulai sesi terminal baru.

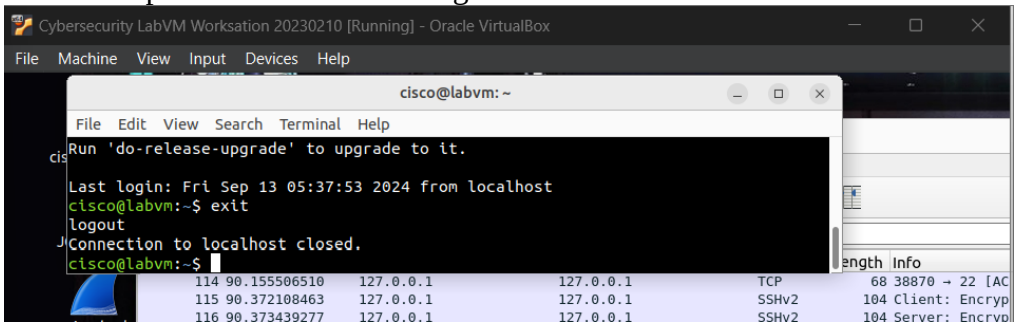


c. Untuk mensimulasikan login SSH, masukkan perintah **ssh localhost** . Jika ini pertama kalinya Anda menggunakan perintah tersebut, sistem akan memperingatkan Anda tentang keaslian localhost dan menanyakan apakah Anda ingin melanjutkan. Masukkan **yes** , lalu **password** sebagai kata sandi untuk login.

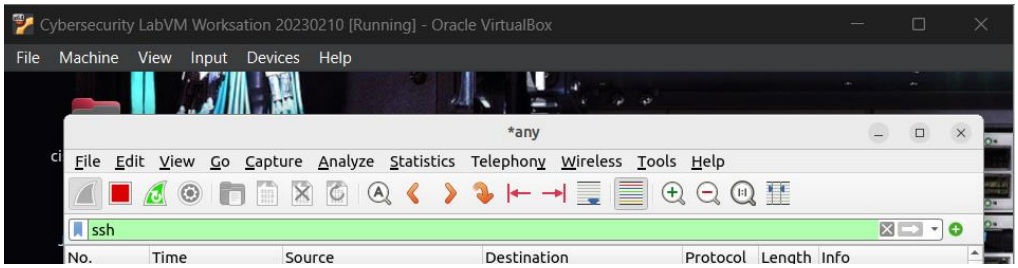
cisco@labvm:~$ **ssh lokalhost**
Keaslian host 'localhost (::1)' tidak dapat dipastikan.
Sidik jari kunci ECDSA adalah SHA256:lEvtfM55v9O8L88uvZ4Em/UL4ARo8jWGE1hV8mVnDhQ.
Apakah Anda yakin ingin terus menghubungkan (ya/tidak/[sidik jari])? **ya**
Peringatan: 'localhost' (ECDSA) telah ditambahkan secara permanen ke daftar host yang diketahui.
kata sandi cisco@localhost: **kata sandi**
Selamat datang di Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)
 * Dokumentasi: https://help.ubuntu.com
 * Manajemen: https://landscape.canonical.com
 * Dukungan: https://ubuntu.com/advantage
0 pembaruan dapat segera diinstal.
0 dari pembaruan ini adalah pembaruan keamanan.
Login terakhir: Kamis 25 Mar 14:01:58 2021 dari localhost
cisco@labvm:~$



d. Masukkan perintah **exit** untuk mengakhiri sesi SSH.



e. Kembali ke Wireshark dan hentikan penangkapan. Jika Anda meninggalkan **telnet** sebagai istilah pencarian di kolom **Apply a display filter** , tidak ada paket yang akan dicantumkan. Ubah istilah pencarian dari **telnet** ke **ssh** . Semua paket dari sesi SSH Anda sekarang akan ditampilkan di panel **Packet List** .



f. Di panel **Rincian Paket** , perluas bidang **Protokol SSH** untuk melihat konten. Di panel **Daftar Paket** , klik paket pertama, lalu gunakan panah bawah untuk melihat berbagai paket SSH. Perhatikan bahwa bidang **Data** untuk **Protokol SSH** menunjukkan bahwa semua data dienkripsi.