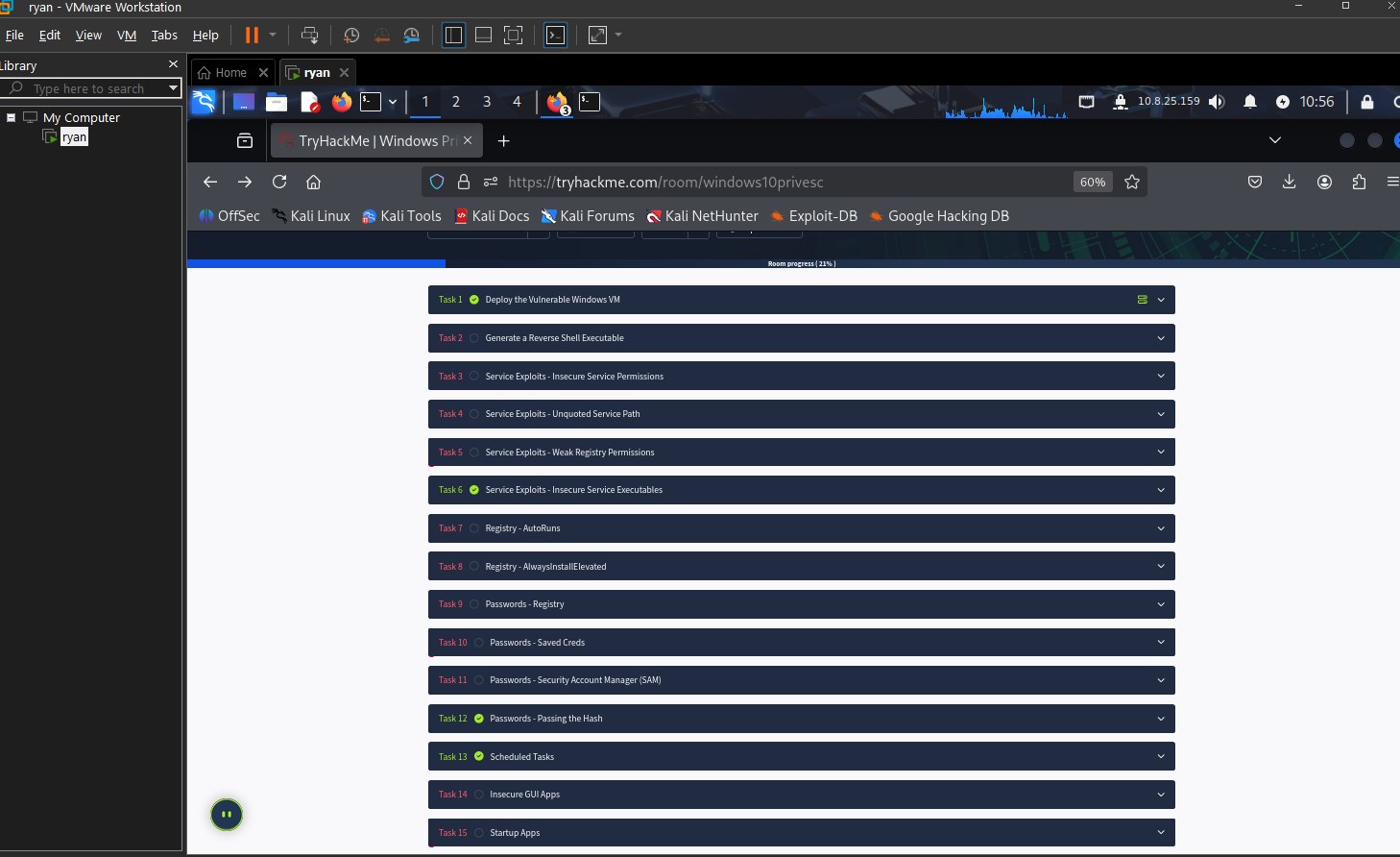


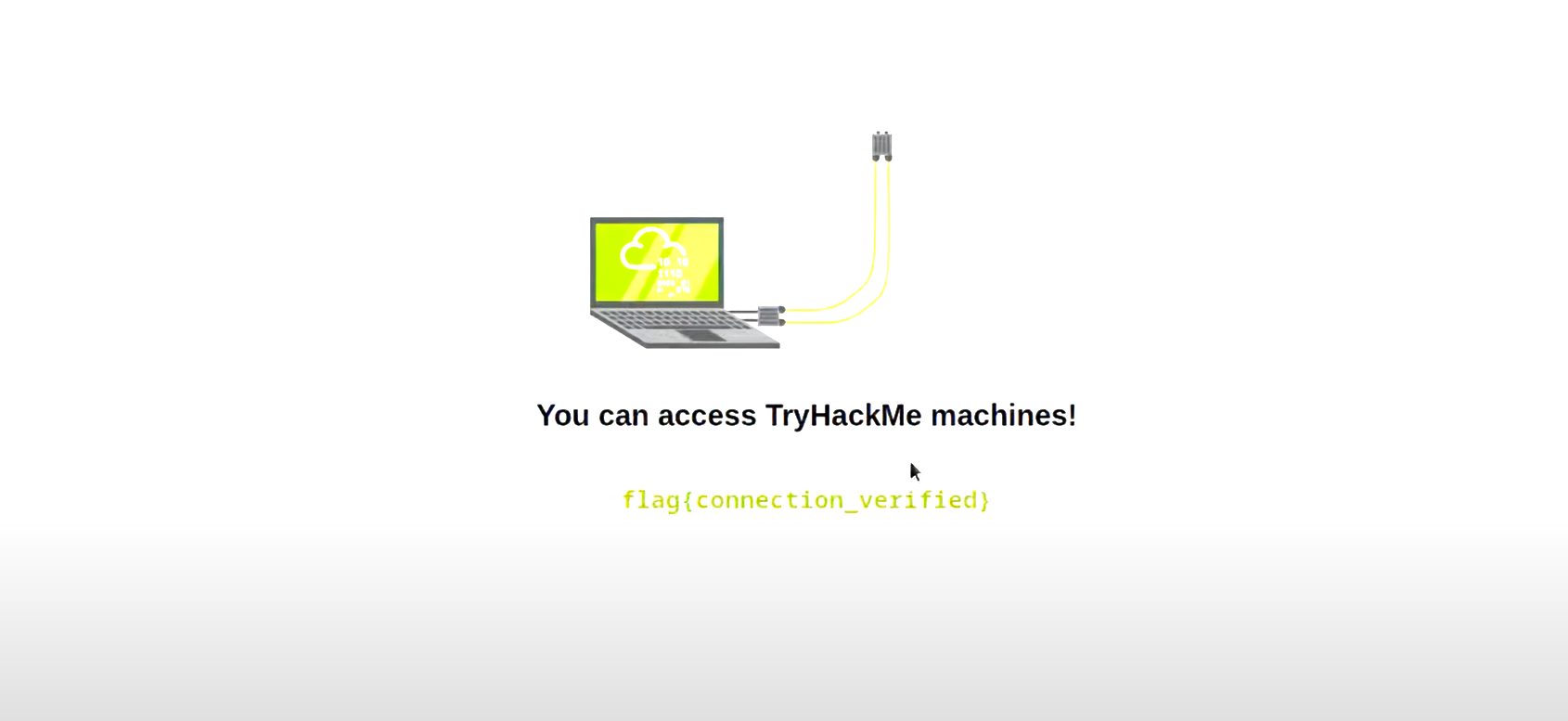
**Beberapa contoh umum untuk sistem Linux adalah:**

***Menambahkan SSH Key Publik***: Setelah mendapatkan akses root, kita bisa menambahkan SSH key publikmu ke file ~/.ssh/authorized\_keys milik pengguna root. Ini akan memungkinkan untuk melakukan login sebagai root langsung tanpa memerlukan kata sandi

***Membuat Cron Job***: Kamu bisa membuat cron job yang berjalan pada interval tertentu (misalnya, setiap kali sistem boot) yang akan menjalankan perintah tertentu, seperti membuat reverse shell kembali ke mesin

***Modifikasi Service Systemd***: Kita dapat membuat atau memodifikasi layanan systemd agar payload berbahaya berjalan secara otomatis saat sistem menyala



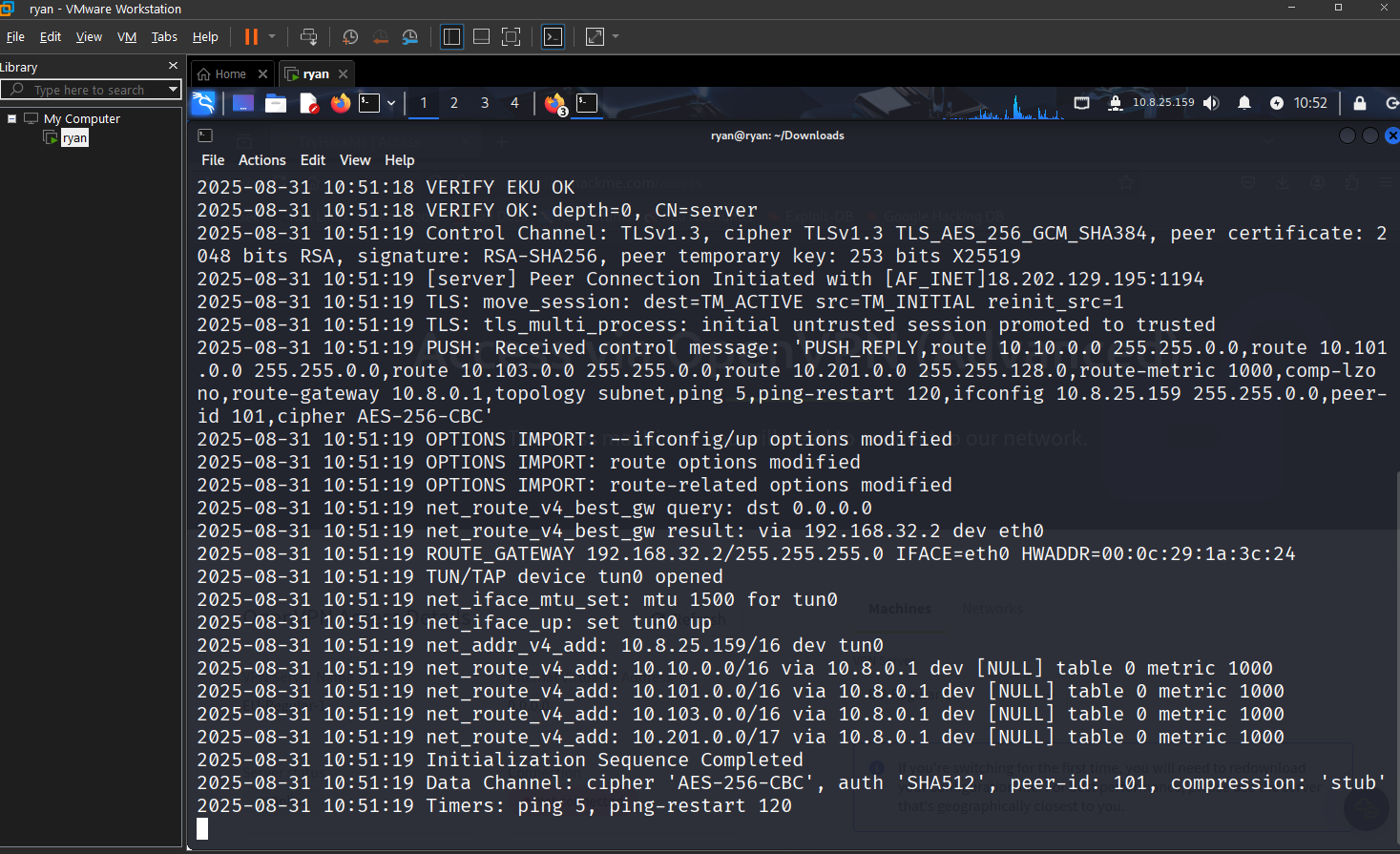


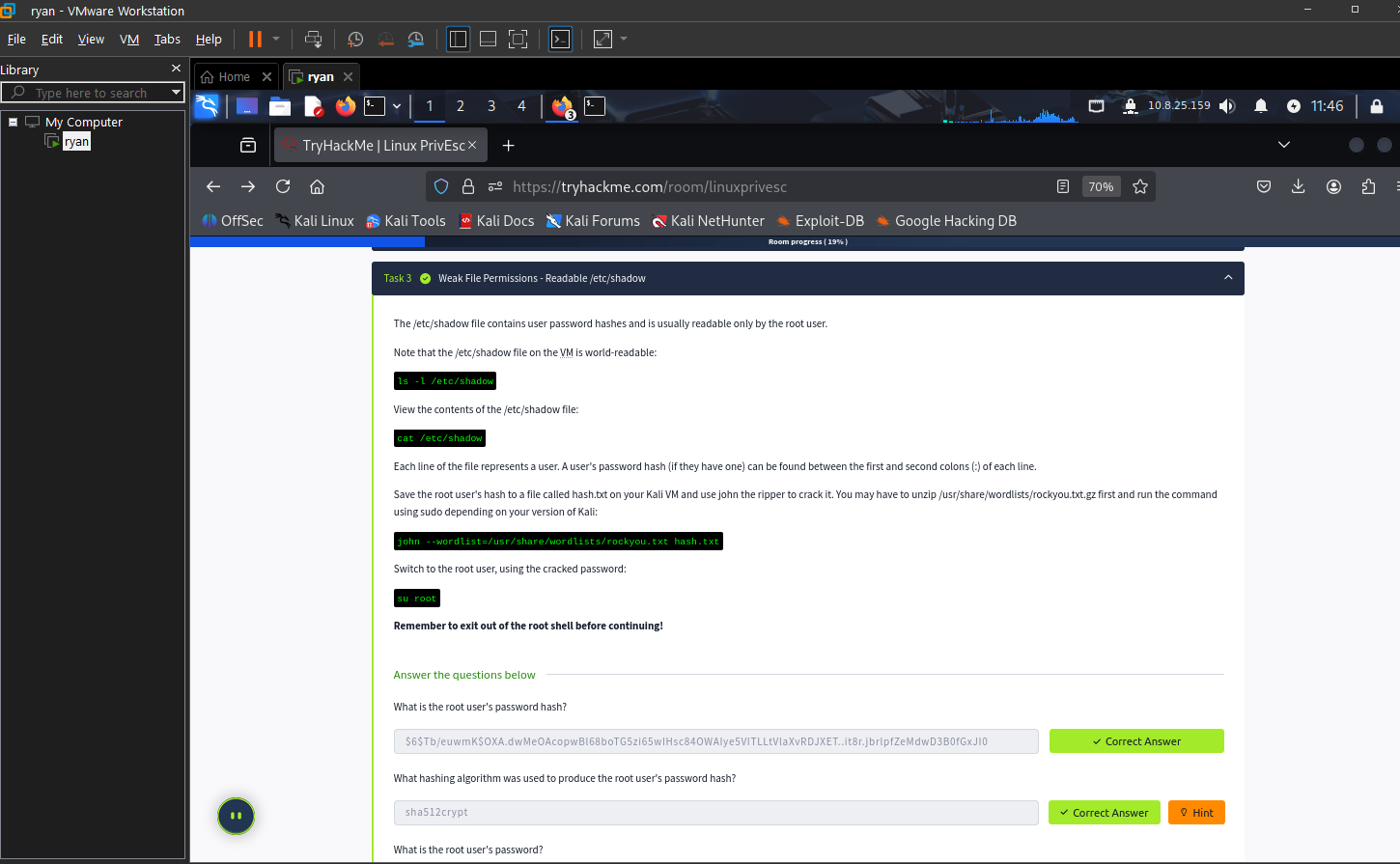
***Cyber Kill Chain***

**1. Delivery (Pengiriman) & Exploitation (Eksploitasi)**

Pada fase ini, tujuan penyerang adalah mengirimkan payload dan mengeksploitasi kerentanan untuk mendapatkan akses awal ke sistem target. Langkah yang harus lakukan: Kita dapat menggunakan perintah ssh untuk mencoba terhubung ke server Debian. Perintah ini adalah alat pengiriman (delivery) yang membawa permintaan koneksi ke server

**Hasil**: Setelah mengatasi kesalahan koneksi dan memasukkan kata sandi yang benar, kita berhasil mendapatkan akses ke server sebagai pengguna user. Ini adalah eksploitasi awal (initial exploitation) yang berhasil, di mana kamu memanfaatkan kerentanan (kata sandi yang lemah) untuk masuk ke dalam sistem

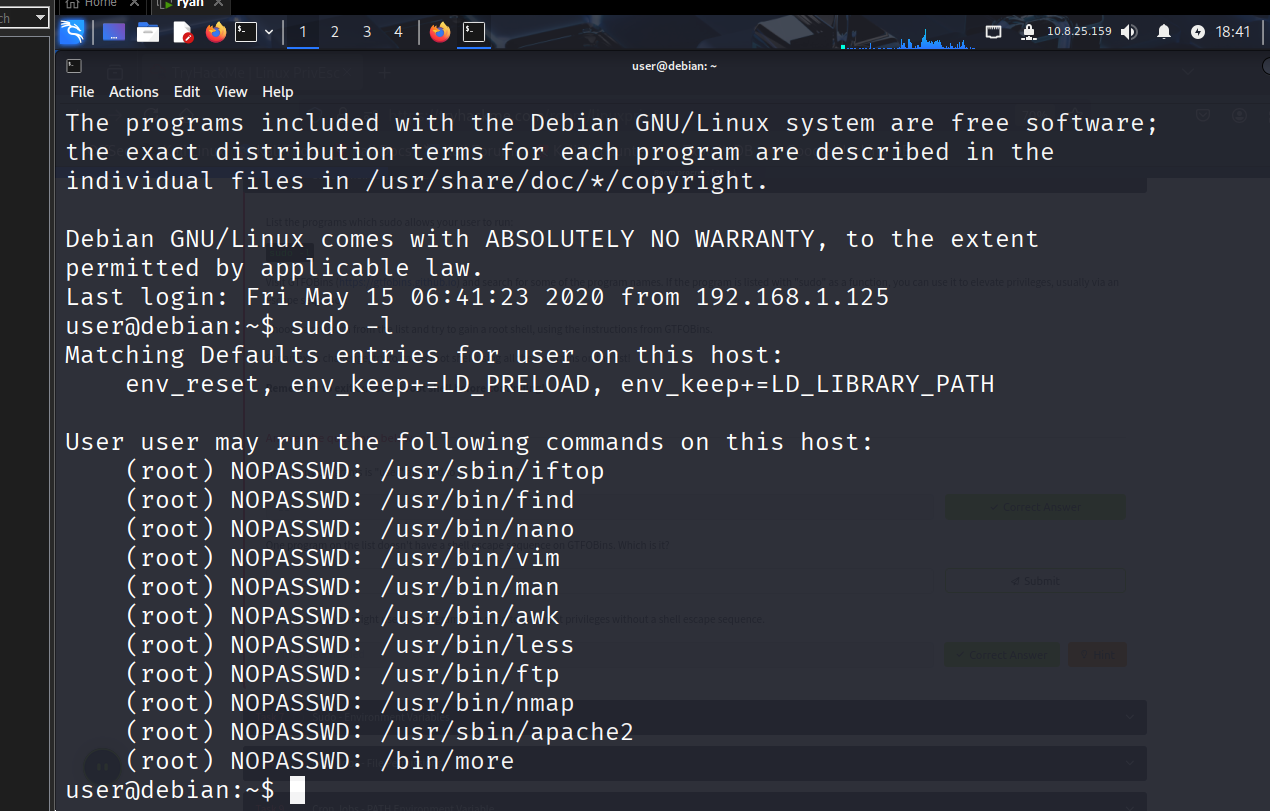




- **id**: Untuk melihat identitas dan grup pengguna saat ini

- **sudo -l**: Untuk mencari tahu program apa saja yang bisa dijalankan dengan sudo tanpa perlu kata sandi

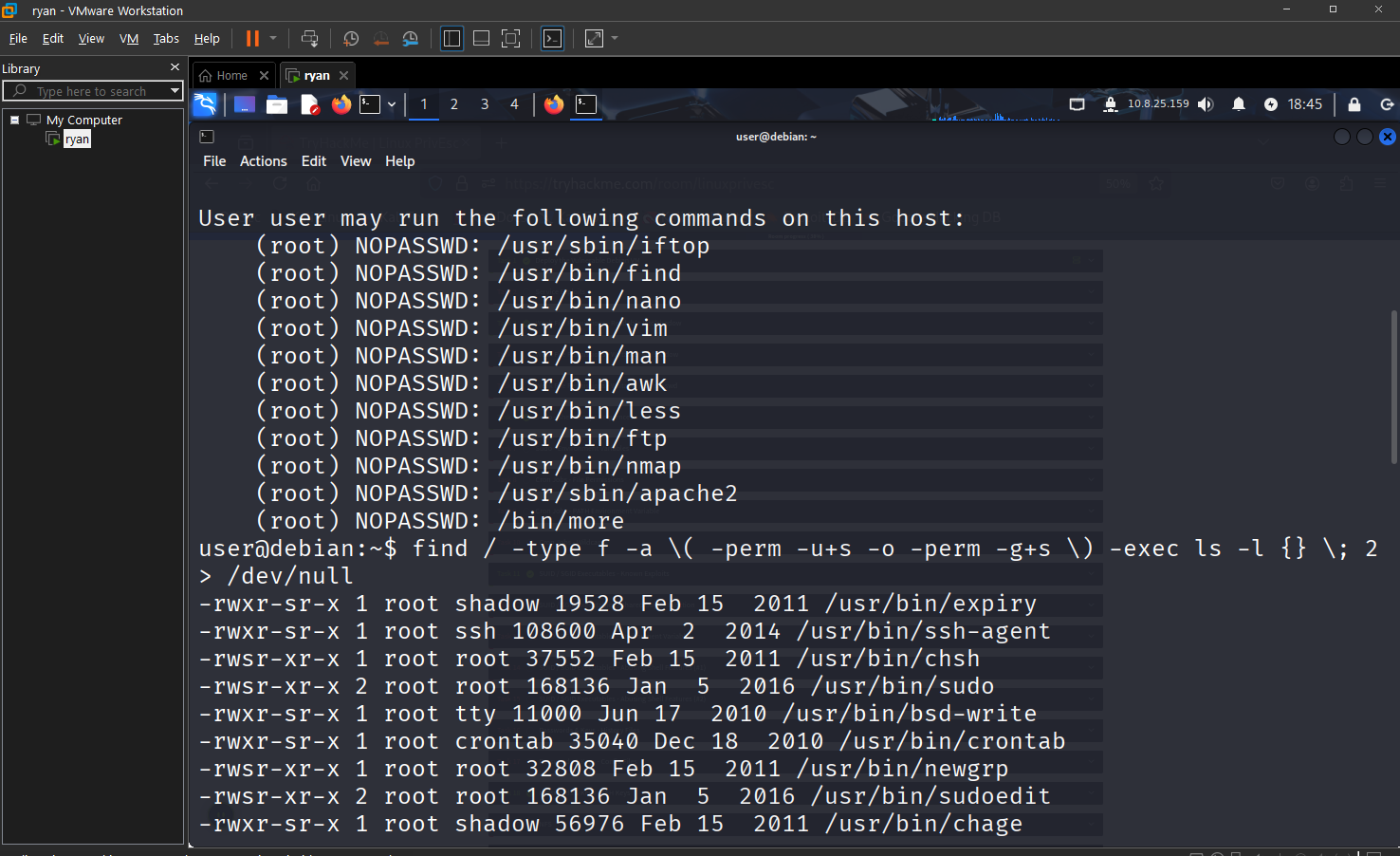
- **cat /etc/shadow**: Untuk melihat daftar pengguna dan hash kata sandi



***Living Off the Land (LoL)***

"**Living Off the Land**" atau disingkat LoL adalah teknik di mana penyerang menggunakan alat atau program yang sudah ada di sistem target, alih-alih mengunggah alat atau malware baru. Tujuan utamanya adalah untuk menghindari deteksi dan menyamarkan aktivitas jahat sebagai aktivitas normal

Contoh: adalah saat kita menggunakan perintah-perintah bawaan seperti **cat**, **id**, dan **sudo** di server Debian untuk mengumpulkan informasi dan melakukan peningkatan hak akses



***Pengertian Privilege Escalation:***

**Privilege escalation** adalah proses di mana seorang penyerang, yang sudah memiliki akses awal ke sistem (misalnya sebagai pengguna biasa), berusaha untuk mendapatkan hak akses yang lebih tinggi. Tujuannya adalah untuk menjadi administrator atau root, sehingga mereka bisa melakukan hampir semua hal di sistem, seperti mengubah konfigurasi, menginstal program, atau menghapus file penting

**Jenis-jenisnya**

Peningkatan Hak Akses Vertikal (Vertical Privilege Escalation): Ini adalah jenis yang paling umum dalam tugas ini. Ini terjadi ketika kamu beralih dari akun dengan hak akses rendah (seperti pengguna biasa user di server Debian) ke akun dengan hak akses tertinggi, yaitu root.

Peningkatan Hak Akses Horizontal (Horizontal Privilege Escalation): Ini terjadi ketika kita mendapatkan akses ke akun pengguna lain di sistem yang memiliki hak akses setara denganmu. Contohnya, pengguna ryan dan berhasil mendapatkan akses ke akun pengguna admin (tanpa menjadi root)

**2. Post-Exploitation & Privilege Escalation (Peningkatan Hak Akses)**

Setelah mendapatkan akses awal, penyerang akan melakukan tindakan pasca-eksploitasi untuk mengumpulkan informasi lebih lanjut dan meningkatkan hak aksesnya

**Langkah yang kita lakukan:**

Kita menjalankan perintah sudo -l di server untuk mengumpulkan informasi tentang hak akses yang dimiliki pengguna user. kemudian menggunakan perintah cat /etc/shadow untuk melihat isi file sensitif tersebut. John the Ripper untuk memecahkan hash kata sandi root yang kamu dapatkan

**Hasil**: Mendapatkan kata sandi root dan beralih ke shell root adalah sebuah contoh langsung dari peningkatan hak akses vertikal (vertical privilege escalation) yang merupakan bagian krusial

