**BASELINE AUTOMATED SECURITY HARDENING PADA UBUNTU SERVER MENGGUNAKAN TOOLS OPENSCAP DAN ANSIBLE**

|  |  |
| --- | --- |
| **DISUSUN OLEH** | |
| **NAMA** | Haldi Alfiansyach |
| **CONTACT / MORE INFO** | https://www.linkedin.com/in/haldialf |

**DAFTAR ISI**

[PENGENALAN TOOLS OPENSCAP 1](#_Toc178813488)

[CARA PENGGUNAAN TOOLS OPENSCAP 2](#_Toc178813489)

[1. Instalasi OpenSCAP pada OS Linux 2](#_Toc178813490)

[2. Instalasi SCAP Security Guide untuk mendapatkan profile compliance check 2](#_Toc178813491)

[3. List OpenSCAP Profile 2](#_Toc178813492)

[4. Compliance Check dengan menggunakan template SCAP 2](#_Toc178813493)

[5. Pengubahan format pada hasil check compliance dari xml menjadi html 3](#_Toc178813494)

[PENGENALAN TOOLS ANSIBLE 5](#_Toc178813495)

[Fungsi Utama Ansible: 5](#_Toc178813496)

[1. Manajemen Konfigurasi: 5](#_Toc178813497)

[2. Deployment Aplikasi: 5](#_Toc178813498)

[3. Orkestrasi: 5](#_Toc178813499)

[Fitur Utama Ansible: 5](#_Toc178813500)

[Komponen Penting dalam Ansible: 6](#_Toc178813501)

[1. Playbook: 6](#_Toc178813502)

[2. Inventory: 6](#_Toc178813503)

[3. Modules: 6](#_Toc178813504)

[4. Roles: 6](#_Toc178813505)

[5. Tasks: 6](#_Toc178813506)

[CARA PENGGUNAAN TOOLS ANSIBLE 7](#_Toc178813507)

[1. Instalasi Ansible pada Linux 7](#_Toc178813508)

[2. Instalasi Ansible Galaxy pada Linux 7](#_Toc178813509)

[3. Cek List Ansible Playbook yang didapat dari Ansible Galaxy 7](#_Toc178813510)

[4. Isi Ansible Playbook 7](#_Toc178813511)

[5. Buat file bernama inventory.ini dalam folder List Ansible Playbook yang sudah di Install 7](#_Toc178813512)

[6. Hardening ke server target dengan metode SSH 7](#_Toc178813513)

# PENGENALAN TOOLS OPENSCAP

OpenSCAP adalah sebuah framework open source yang digunakan untuk melakukan evaluasi, pengukuran, dan penegakan kebijakan keamanan pada sistem komputer. Beberapa poin penting tentang OpenSCAP:

1. **Tujuan:** OpenSCAP membantu organisasi memeriksa konfigurasi keamanan sistem mereka secara otomatis dan memastikan kepatuhan terhadap standar keamanan tertentu.
2. **Standar:** OpenSCAP mendukung berbagai standar keamanan, termasuk CIS (Center for Internet Security) Benchmarks.
3. **Fungsi:** Tools ini dapat melakukan pemindaian sistem, mengidentifikasi kerentanan, dan memberikan laporan tentang status kepatuhan keamanan.
4. **Otomatisasi:** OpenSCAP memungkinkan otomatisasi proses audit keamanan, yang sangat membantu dalam mengelola keamanan sistem skala besar.
5. **Integrasi:** Dapat diintegrasikan dengan berbagai sistem dan alat manajemen keamanan lainnya.

Kaitannya dengan CIS Benchmark:

* CIS Benchmarks adalah serangkaian praktik terbaik yang diakui secara internasional untuk mengamankan sistem IT.
* OpenSCAP dapat menggunakan profil keamanan berdasarkan CIS Benchmark untuk mengevaluasi apakah sistem Anda mematuhi rekomendasi keamanan tersebut.

Dengan menggunakan OpenSCAP untuk baseline berdasarkan CIS Benchmark, Kita dapat secara efektif dan konsisten menilai dan meningkatkan postur keamanan sistem sesuai dengan standar industri yang diakui.

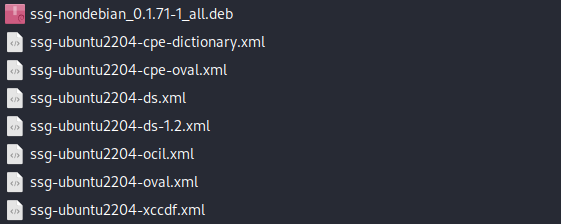
# CARA PENGGUNAAN TOOLS OPENSCAP

## Instalasi OpenSCAP pada OS Linux

sudo apt-get install libopenscap8

## Instalasi SCAP Security Guide untuk mendapatkan profile compliance check

apt install ssg-base ssg-debderived ssg-debian ssg-nondebian ssg-applications

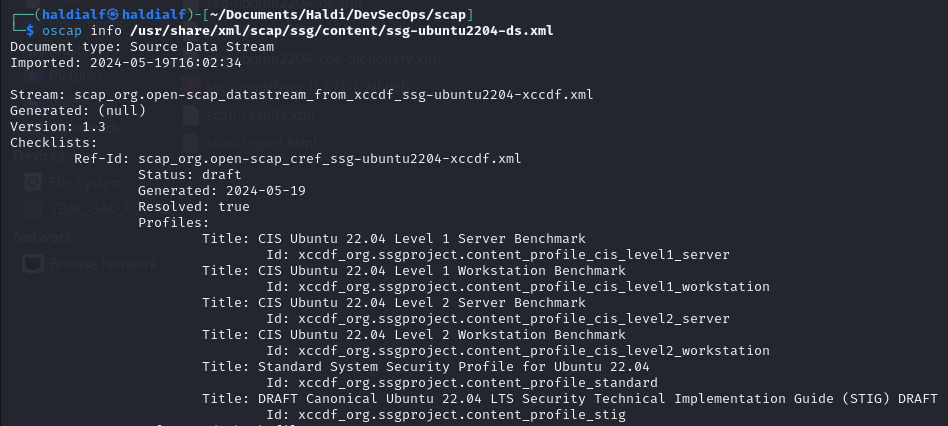


Berikut adalah macam jenis Security Guide yang sudah di download dan install

## List OpenSCAP Profile

oscap info /usr/share/xml/scap/ssg/content/ssg-ubuntu2204-ds.xml

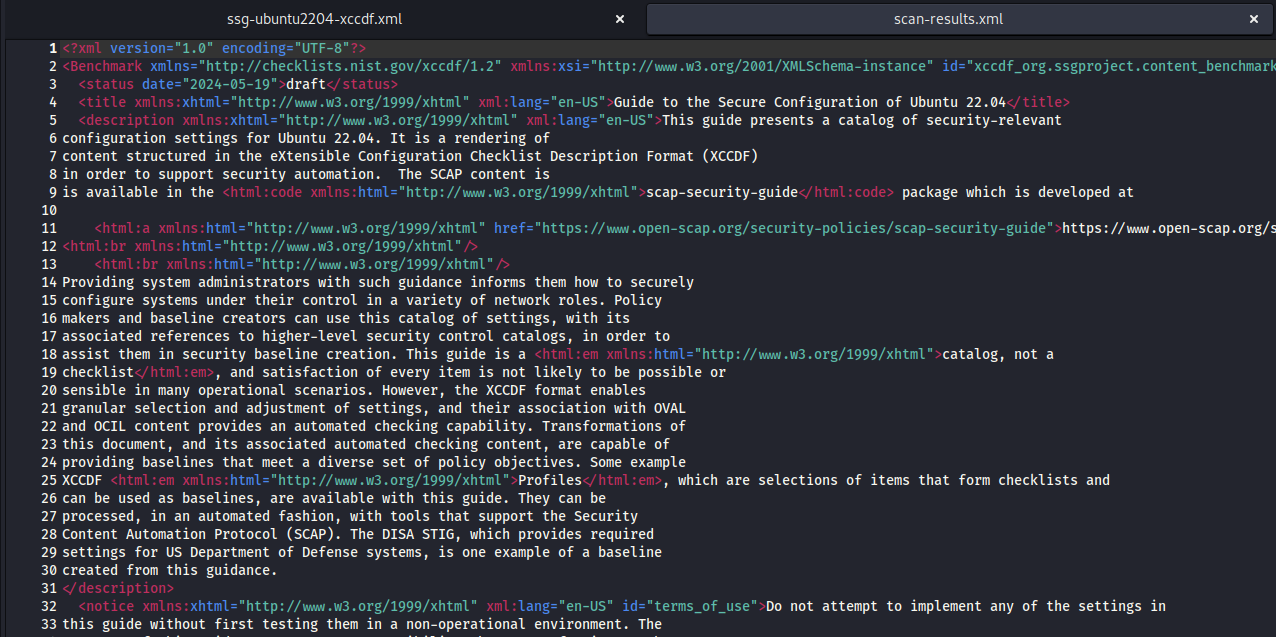
note : ssg-ubuntu2204-ds.xml menunjukkan profile yang akan ditampilkan adalah untuk ubuntu, bisa diubah sesuai dengan kebutuhan server yang akan digunakan



## Compliance Check dengan menggunakan template SCAP

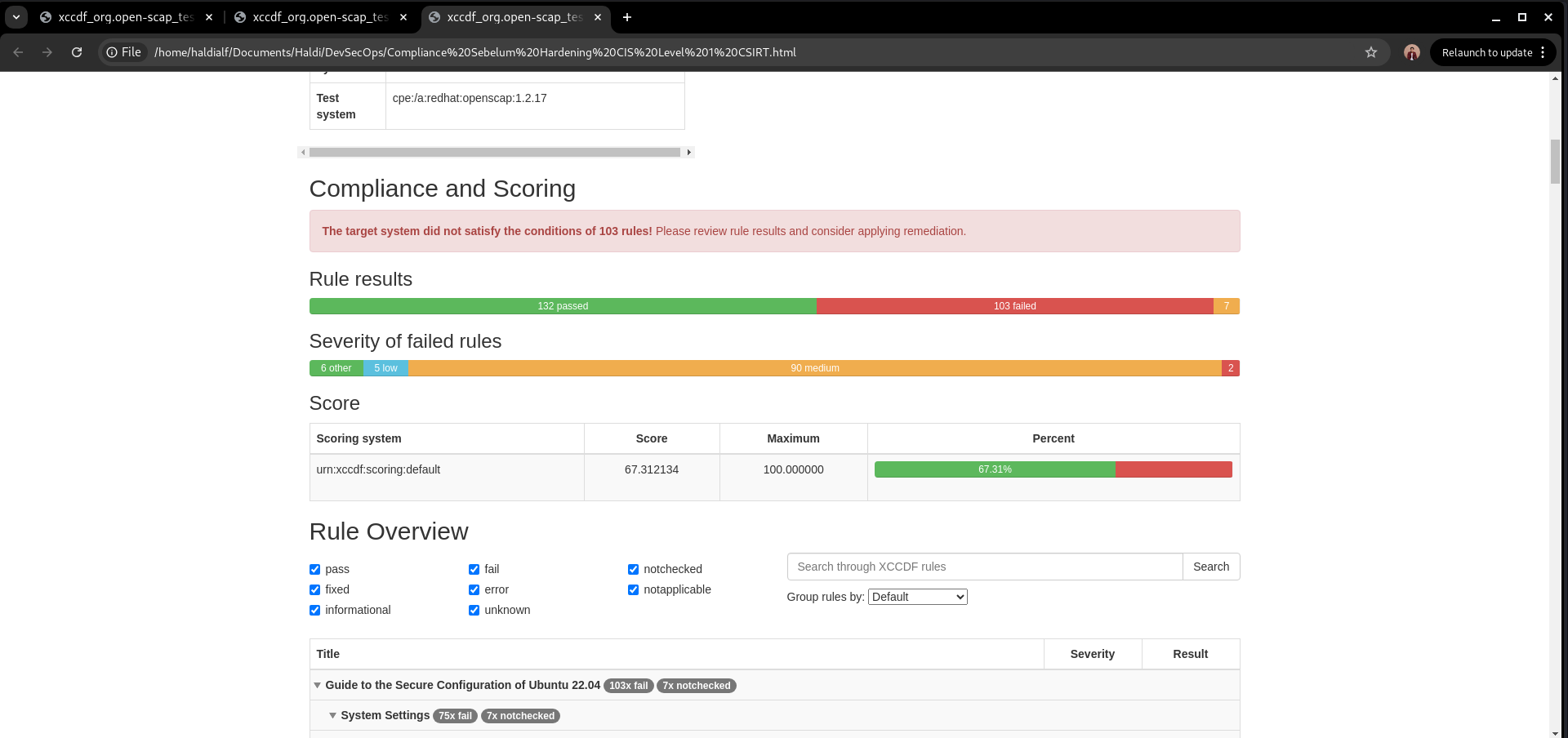
oscap-ssh --sudo intern\_user@192.168.200.207 22 xccdf eval --profile xccdf\_org.ssgproject.content\_profile\_cis\_level1\_server --results scan-results.xml /usr/share/xml/scap/ssg/content/ssg-ubuntu2204-ds.xml

* + intern\_user@192.168.200.207 = user yang akan melakukan SSH ke server target
  + 22 = port
  + xccdf\_org.ssgproject.content\_profile\_cis\_level1\_server = profile yang akan digunakan untuk melakukan compliance check
  + scan-results.xml = memberi nama pada hasil scan result setelah melakukan check compliance

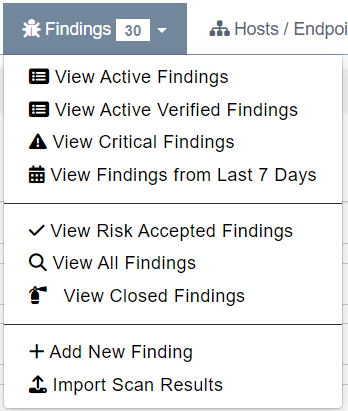


## Pengubahan format pada hasil check compliance dari xml menjadi html

oscap xccdf generate report scan-results.xml > scan-report.html



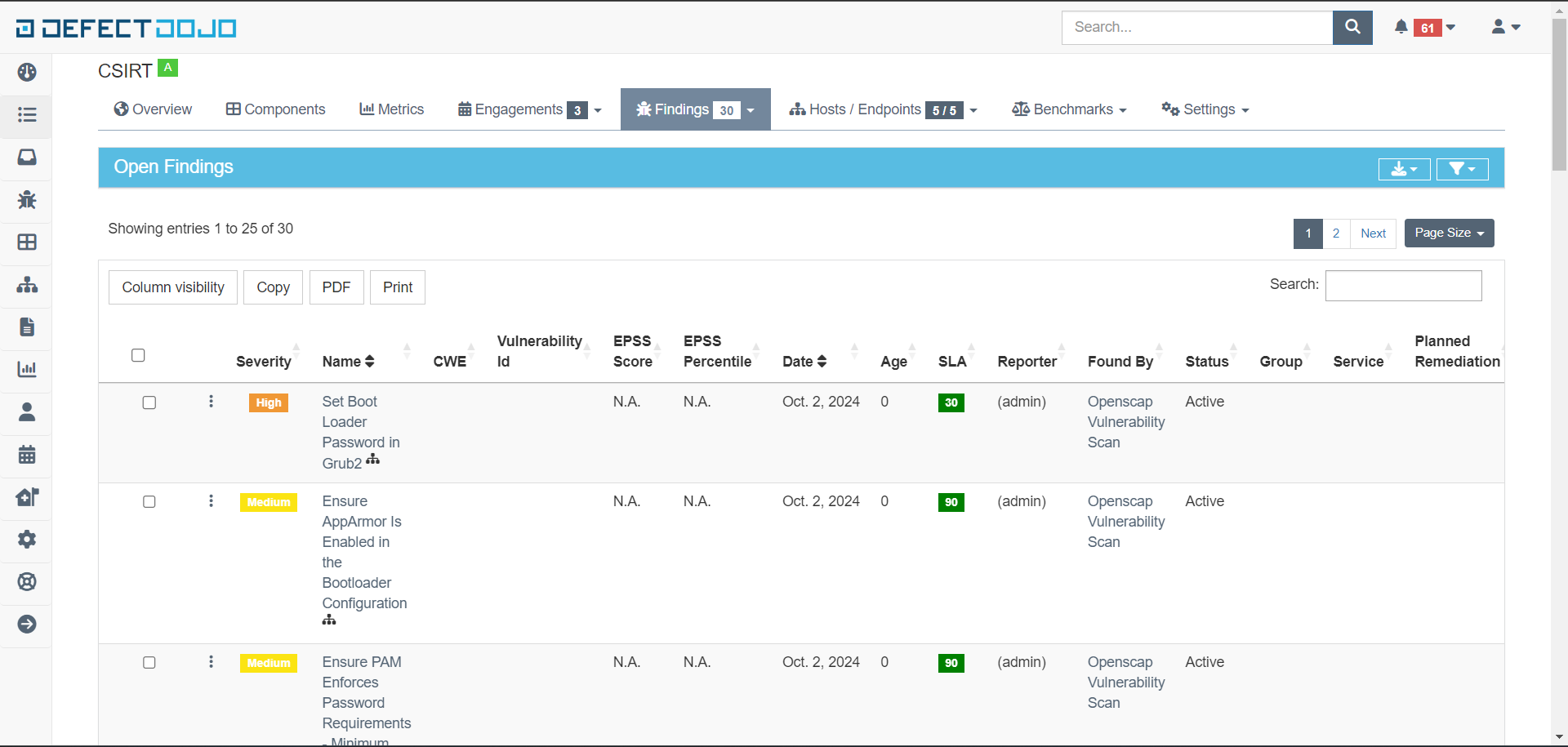
1. **Export Hasil Compliance Check ke DefectDojo**
   * Import scan results pada menu findings



* + Scan type atur menjadi Openscap Vulnerability Scan



* + Akan muncul output seperti ini

****

# PENGENALAN TOOLS ANSIBLE

Ansible adalah alat yang memungkinkan administrator sistem atau DevOps untuk mengotomatisasi berbagai tugas seperti manajemen konfigurasi, instalasi perangkat lunak, dan deployment aplikasi di banyak server atau node secara bersamaan. Semua tugas ini didefinisikan dalam bentuk **playbook** yang menggunakan sintaks sederhana berbasis **YAML**, sehingga mudah dibaca dan dipahami bahkan bagi yang baru mengenal otomasi.

## Fungsi Utama Ansible:

### Manajemen Konfigurasi:

Ansible memungkinkan manajemen konfigurasi server yang konsisten di seluruh infrastruktur. Anda dapat mendefinisikan konfigurasi yang diinginkan dalam playbook Ansible, dan Ansible akan memastikan semua server (node) memenuhi kondisi tersebut.

**Contoh:** Menginstal paket, mengubah file konfigurasi, mengelola pengguna, dan pengaturan izin.

### Deployment Aplikasi:

Dengan Ansible, Anda dapat menyebarkan aplikasi secara otomatis ke satu atau beberapa server. Ini termasuk instalasi perangkat lunak, penyebaran kode aplikasi, pengaturan database, dan konfigurasi layanan pendukung lainnya.

**Contoh:** Menyebarkan aplikasi web ke server yang berbeda dengan satu perintah otomatis.

### Orkestrasi:

Ansible dapat mengkoordinasikan dan mengotomatiskan tugas yang memerlukan eksekusi berurutan pada beberapa server atau layanan. Misalnya, ketika Anda ingin mengelola sistem besar yang terdiri dari berbagai server (database, aplikasi, frontend) yang membutuhkan penanganan berurutan.

**Contoh:** Membangun infrastruktur server secara bertahap, misalnya, provisioning server database sebelum server aplikasi.

## Fitur Utama Ansible:

* **Agentless**: Tidak memerlukan agen khusus untuk dijalankan pada server yang dikelola, cukup SSH atau WinRM.
* **Idempotent**: Ansible hanya melakukan perubahan jika diperlukan, artinya jika server sudah dalam keadaan yang diinginkan, tidak ada tindakan tambahan yang dilakukan.
* **Mudah Digunakan**: Ansible menggunakan sintaks berbasis YAML untuk playbook, yang membuatnya lebih mudah dipahami dan digunakan oleh banyak orang, baik yang memiliki latar belakang teknis maupun tidak.
* **Multiplatform**: Dapat digunakan untuk mengelola berbagai sistem operasi dan perangkat, termasuk Linux, Windows, perangkat jaringan, dan cloud providers seperti AWS, Azure, dan Google Cloud.

## Komponen Penting dalam Ansible:

1. Playbook: File YAML yang mendefinisikan kumpulan tugas dan instruksi yang harus dijalankan oleh Ansible. Playbook menggambarkan secara terperinci apa yang harus dilakukan pada node yang dikelola.
2. Inventory: Daftar server atau node yang akan dikelola oleh Ansible. Inventory bisa berupa file teks sederhana yang mendefinisikan alamat IP atau nama host dari server.
3. Modules: Kumpulan fungsi atau unit kerja yang disediakan oleh Ansible untuk melaksanakan tugas-tugas tertentu, seperti mengelola paket perangkat lunak, menjalankan perintah shell, atau mengelola file.
4. Roles: Struktur direktori yang menyimpan tugas, variabel, dan file yang terkait dengan fungsi atau tujuan tertentu, yang memudahkan pengorganisasian playbook menjadi komponen yang lebih kecil dan modular.
5. Tasks: Perintah atau instruksi individual yang dijalankan oleh Ansible pada node yang dikelola. Task merupakan unit kerja terkecil dalam playbook.

# CARA PENGGUNAAN TOOLS ANSIBLE

## Instalasi Ansible pada Linux

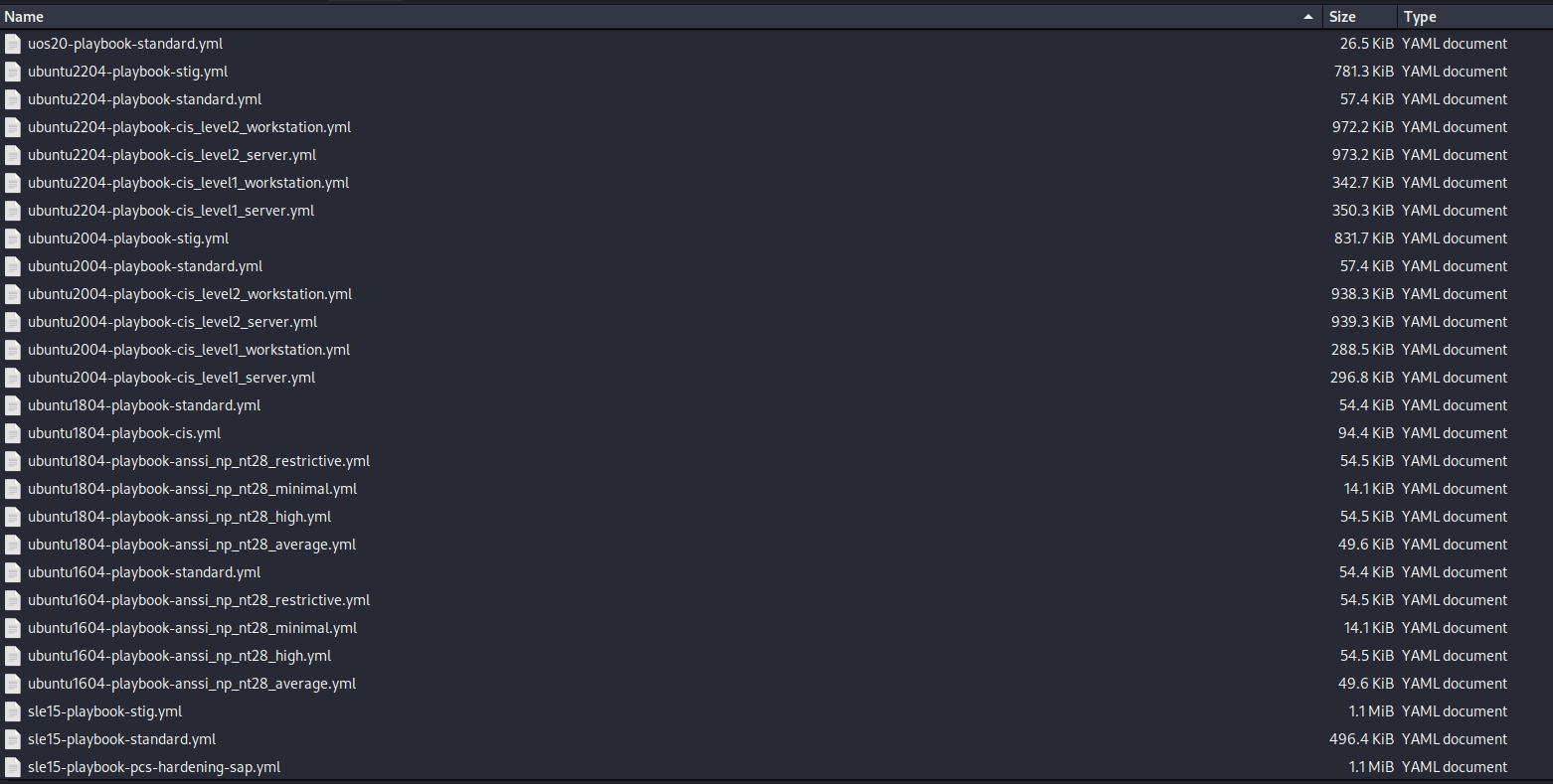
* + sudo apt update
  + sudo apt install ansible

## Instalasi Ansible Galaxy pada Linux

* + ansible-galaxy install dev-sec.os-hardening

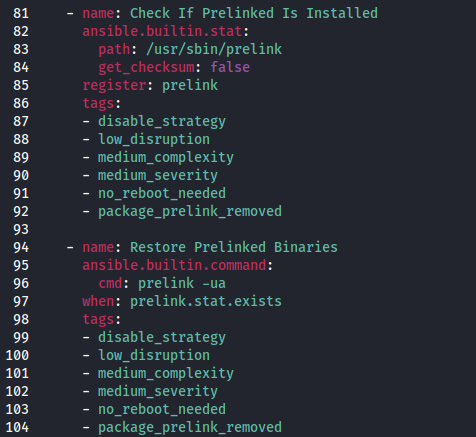
## Cek List Ansible Playbook yang didapat dari Ansible Galaxy

* + Buka folder ansible di direktori penginstalan ansible



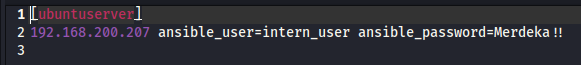
## Isi Ansible Playbook

Isi command yang ada pada ubuntu2204-playbook-cis\_level1\_server

****

## Buat file bernama inventory.ini dalam folder List Ansible Playbook yang sudah di Install

File ini berisi user dan password pada SSH Target



## Hardening ke server target dengan metode SSH

ansible-playbook -i inventory.ini ubuntu2204-playbook-cis\_level1\_server.yml --become --ask-become-pass

* + ubuntu2204-playbook-cis\_level1\_server.yml merupakan profile yang akan digunakan untuk melakukan hardening server dengan CIS Benchmark Level 1
  + Menggunakan Level 1 dikarenakan tidak akan membahayakan server
  + Dapat menggunakan level 2, namun harus disesuaikan dengan environment server



**Penjelasan Status**

* + **ok** : sudah di configure
  + **changed** : baru saja dilakukan konfigurasi
  + **skipped** : dilewatkan karena server target tidak memerlukan konfigurasi tersebut