**LAPORAN PRAKTIKUM III**

**INTRO CYBER SECURITY**

****

**DISUSUN OLEH :**

Nama : Diki Candra

Nim : 2022903430010

Kelas : TRKJ 2B

Jurusan : Teknologi Informasi dan Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Dosen Pembimbing : Atthariq, S.ST, MT

**JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER**

**PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN**

**POLITEKNIK NEGERI LHOKSEUMAWE**

**TAHUN 2023/2024**

**LEMBARAN PENGESAHAN**

Laporan Yang Berjudul : Intro Cyber Security

Disusun Oleh : Diki Candra

Nim : 2022903430010

Jurusan : Teknologi Informasi & Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Mata Kuliah : Databases Aplication

Tanggal Praktikum : 19 Oktober 2023

Tabel Penilaian : :

Mengetahui ,

Dosen Pembimbing, Penyusun,

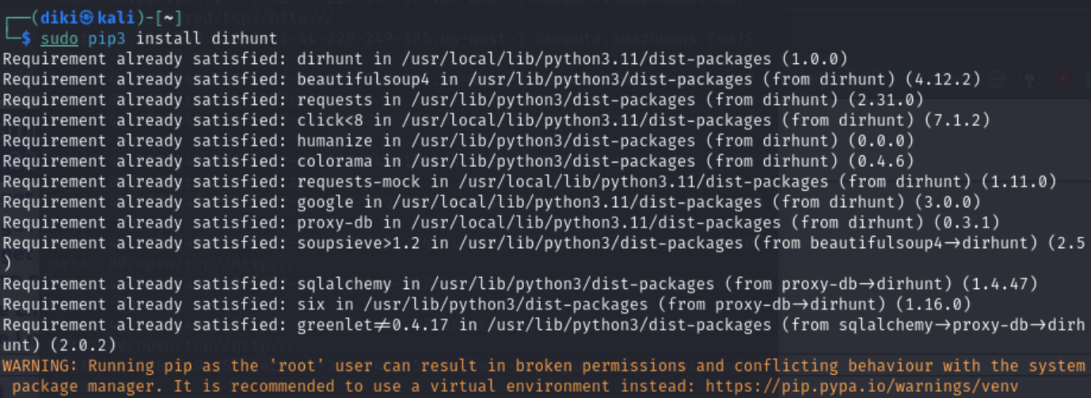
Atthariq, S.ST, MT Diki Candra

NIP 197807242001121001 NIM 2022903430010

**LANGKAH PERCOBAAN DAN HASIL PERCOBAAN**

1. Langkah pertama install dirhunt terlebih dahulu

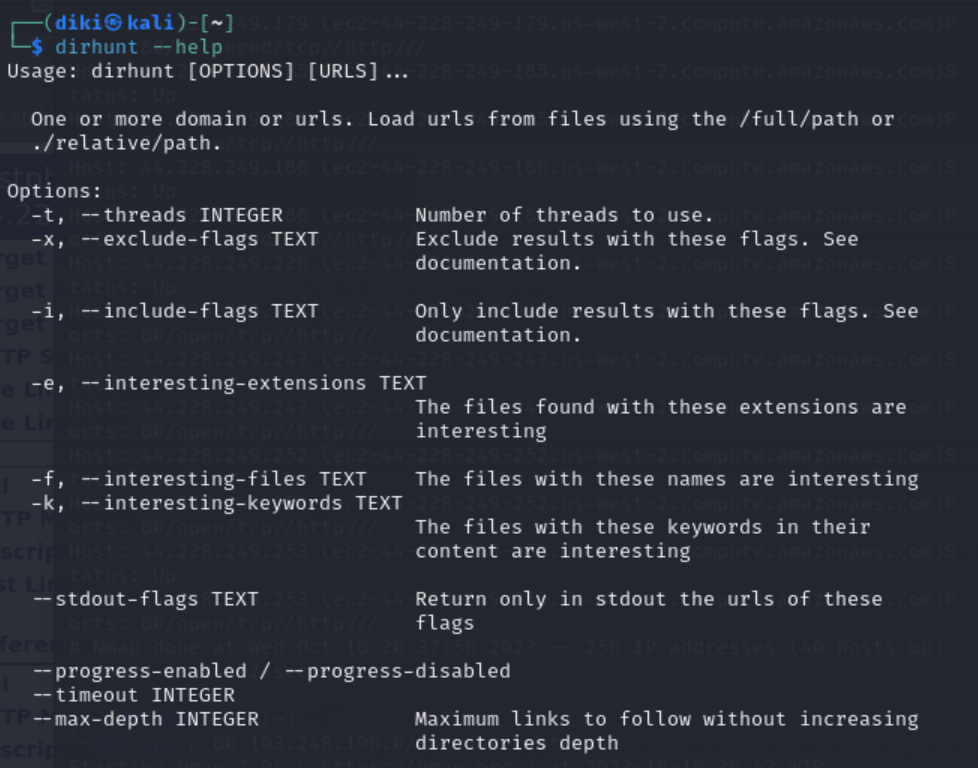
$ sudo pip3 install dirhunt

****

**Penjelasan :**

Mendownload tool dirhunt.

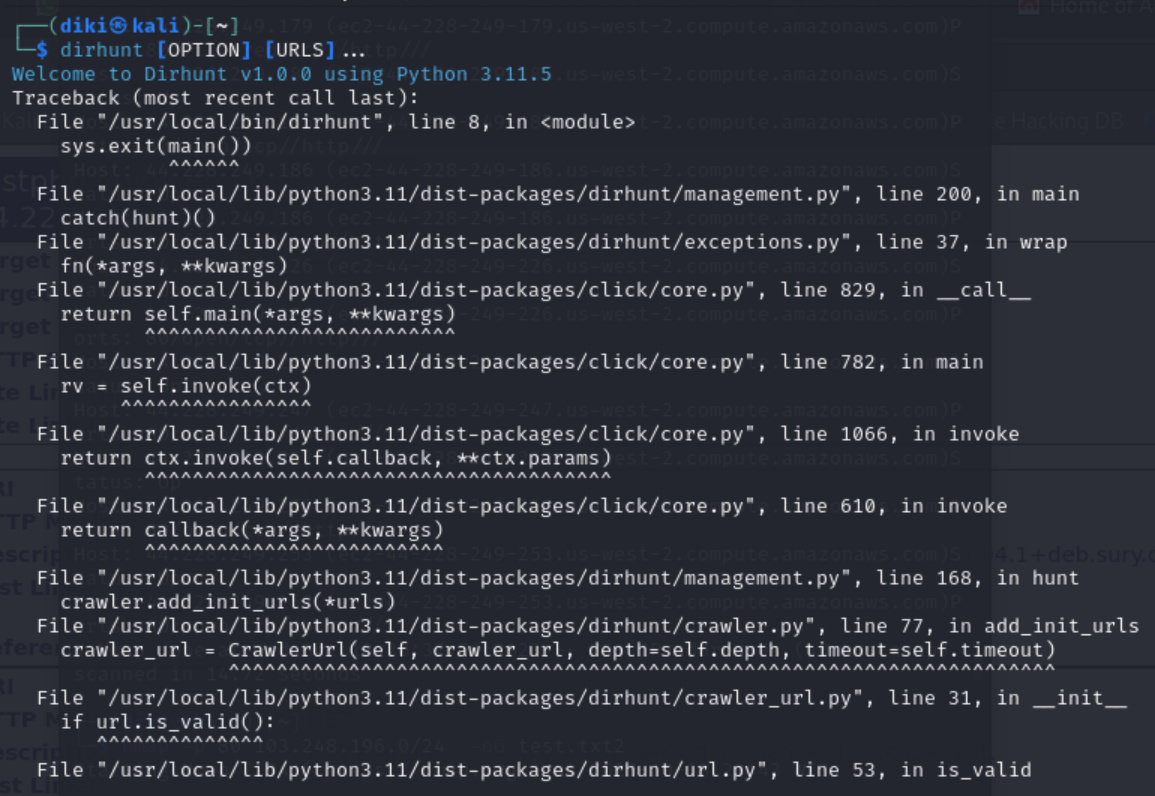
1. Selanjutnya ketik $ dirhunt --help



Penjelasan :

Perintah **dirhunt --help** digunakan untuk menampilkan bantuan atau panduan singkat tentang cara menggunakan alat atau perangkat lunak "dirhunt".

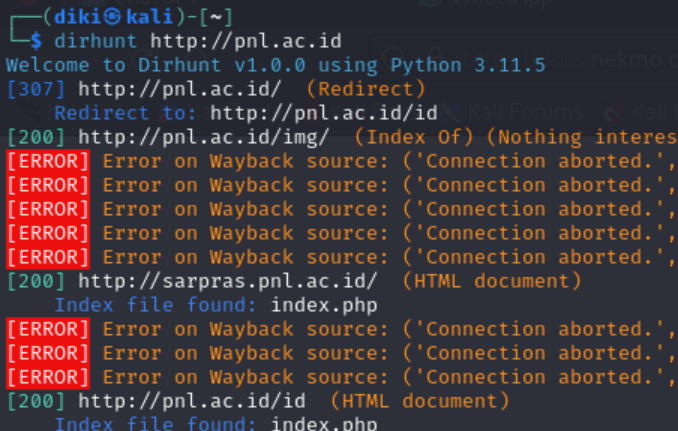
1. Selanjutnya ketik $ dirhunt [OPTIONS] [URLS]…



Penjelasan :

Perintah **dirhunt [OPTIONS] [URLS]…** digunakan untuk melakukan pemindaian otomatis direktori dan file pada situs web yang ditentukan. Itu membantu dalam pengujian keamanan dan penemuan struktur situs web.

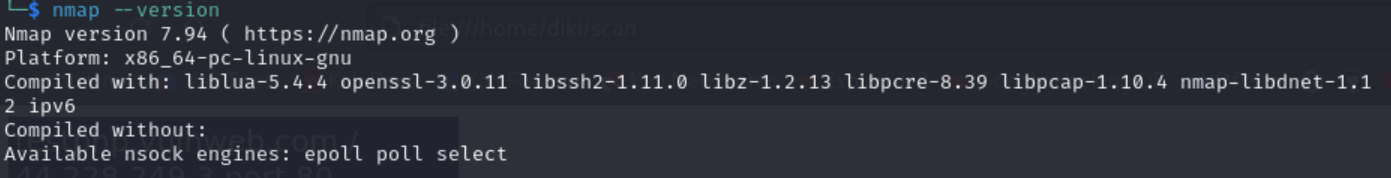
1. Lakukan perintah $ dirhunt <http://pnl.ac.id> untuk melihat sebuah direktori dalam sebuah website.



Penjelasan :

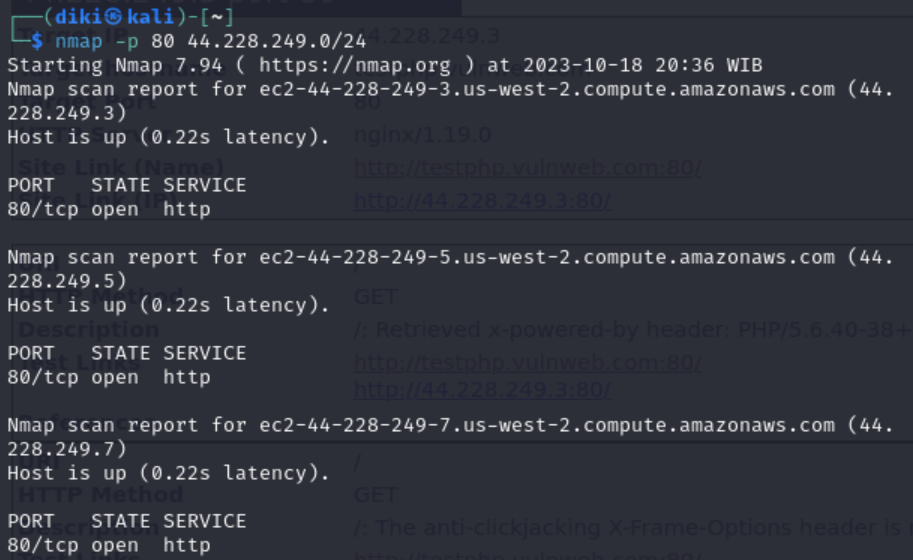
Di bawah ini adalah penjelasan singkat mengenai beberapa hasil pemindaian yang tercantum:

1. **[307]** <http://pnl.ac.id/> (Redirect): Ini adalah URL yang mengalami pengalihan ke lokasi lain, yaitu <http://pnl.ac.id/id>.
2. **[200]** <http://pnl.ac.id/img/> (Index Of): Ini adalah URL yang mengizinkan indeks isi direktori (Index Of). Dalam hal ini, tidak ada informasi menarik yang ditemukan dalam direktori tersebut.
3. **[ERROR] Error on Wayback source**: Terdapat beberapa kesalahan saat mencoba mengakses sumber Wayback, yang mungkin merupakan layanan referensi untuk arsip web.
4. **[200]** <http://sarpras.pnl.ac.id/> (HTML document): Ini adalah URL yang mengandung dokumen HTML. Di sini, file indeks "index.php" ditemukan.
5. **[200]** <http://pnl.ac.id/id> (HTML document): Ini adalah URL lain yang mengandung dokumen HTML, dan juga memiliki file indeks "index.php".
6. **[200]** <http://pnl.ac.id/en/> (HTML document): Ini adalah URL lain yang mengandung dokumen HTML.
7. **[301]** [http://www.pnl.ac.id:80/](http://www.pnl.ac.id/) (Redirect): Ini adalah URL lain yang mengalami pengalihan ke <http://pnl.ac.id/id>.
8. **[200]** <http://kimia.pnl.ac.id/> (HTML document): Ini adalah URL yang mengandung dokumen HTML, dan juga memiliki file indeks "index.php".
9. **[301]** <http://elektro.pnl.ac.id/> (Redirect): Ini adalah URL lain yang mengalami pengalihan.
10. Lakukan perintah $ namp -version untuk mengecek tool nmap dalam versi berapa



1. Untuk mengecek ip target yang keluar dari network kalkulator ketikan

$ namp -p 80 44.228.249.0/24



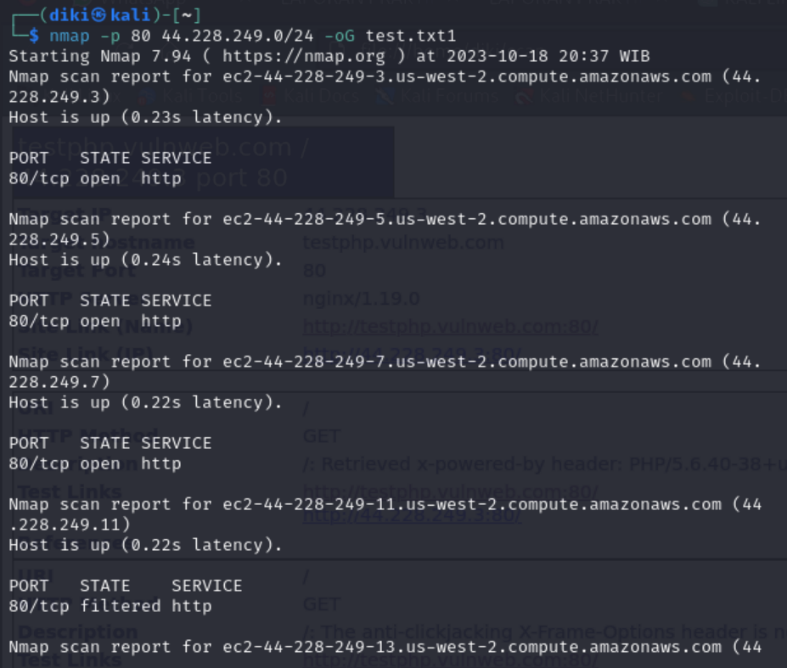
Penjelasannya:

Di sini, beberapa informasi penting yang dapat diambil dari laporan pemindaian ini:

* **Versi Nmap**: Versi Nmap yang digunakan adalah 7.94, dan pemindaian dilakukan pada tanggal 18 Oktober 2023 pada pukul 20:37 WIB.
* **Alamat IP Host**: Ada beberapa host yang dipindai dengan alamat IP yang berbeda. Sejumlah host ditemukan dalam kisaran alamat IP 44.228.249.x.
* **Status Host**: Pemindaian menunjukkan status host. Host yang "up" berarti host tersebut dapat dijangkau dalam jaringan (memiliki respon), sedangkan host yang "filtered" berarti pemindaian port gagal atau diblokir.
* **Port 80**: Pemindaian port menunjukkan bahwa port 80 (HTTP) terbuka di sebagian besar host yang "up." Ini menunjukkan bahwa host-host ini memiliki layanan web HTTP yang aktif.
* **Latensi**: Latensi adalah waktu respons yang diperlukan oleh host. Dalam pemindaian ini, host-host ini memiliki latensi berkisar antara 0.21 hingga 0.24 detik.

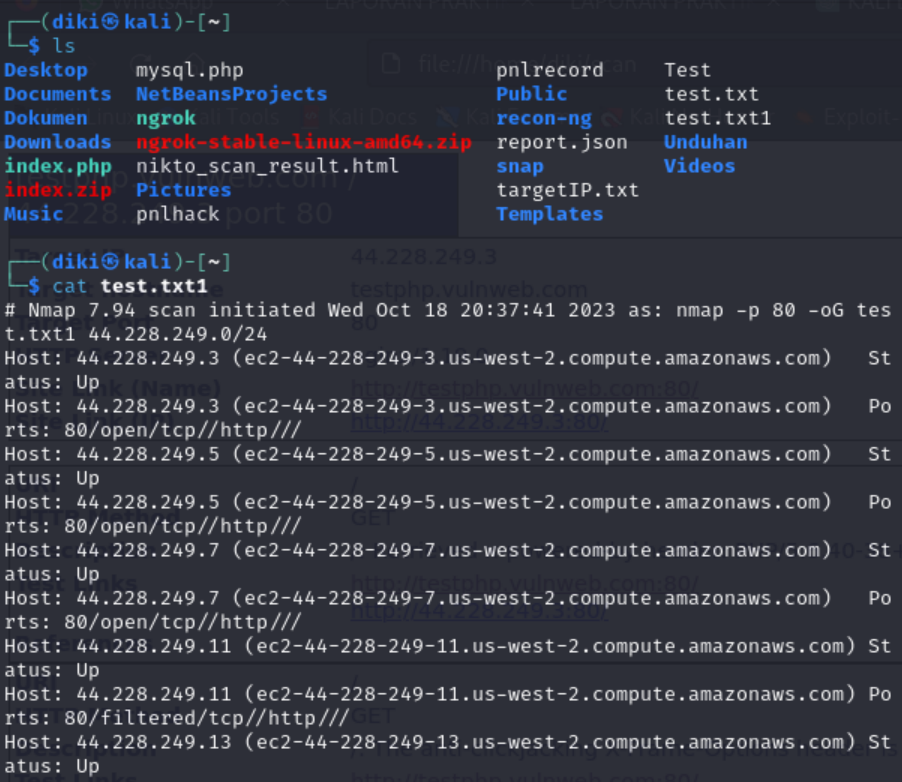
Pemindaian ini memberikan gambaran umum tentang host dan port yang tersedia dalam jaringan yang dipindai pada saat pemindaian dilakukan. Port 80 terbuka pada sebagian besar host, menunjukkan ketersediaan layanan web HTTP di host-host ini.

1. Berikut cara untuk menyimpan informasi setelah melakukan scanning dengan perintah $ nmap -p 80 44.228.249.0/24 -oG test.txt1



Ketik $ ls untuk melihat apakah ada file yang sudah di buat dan ketik $

cat test.txt1 untuk melihat atau membuka file text.txt1



Lakukan perintah $ cat test.txt1 untuk melihat isi scanning yang sudah di lakukan.

1. Selanjutnya ketik $ nikto -Tuning 9 -h http://testphp.vulweb.com/

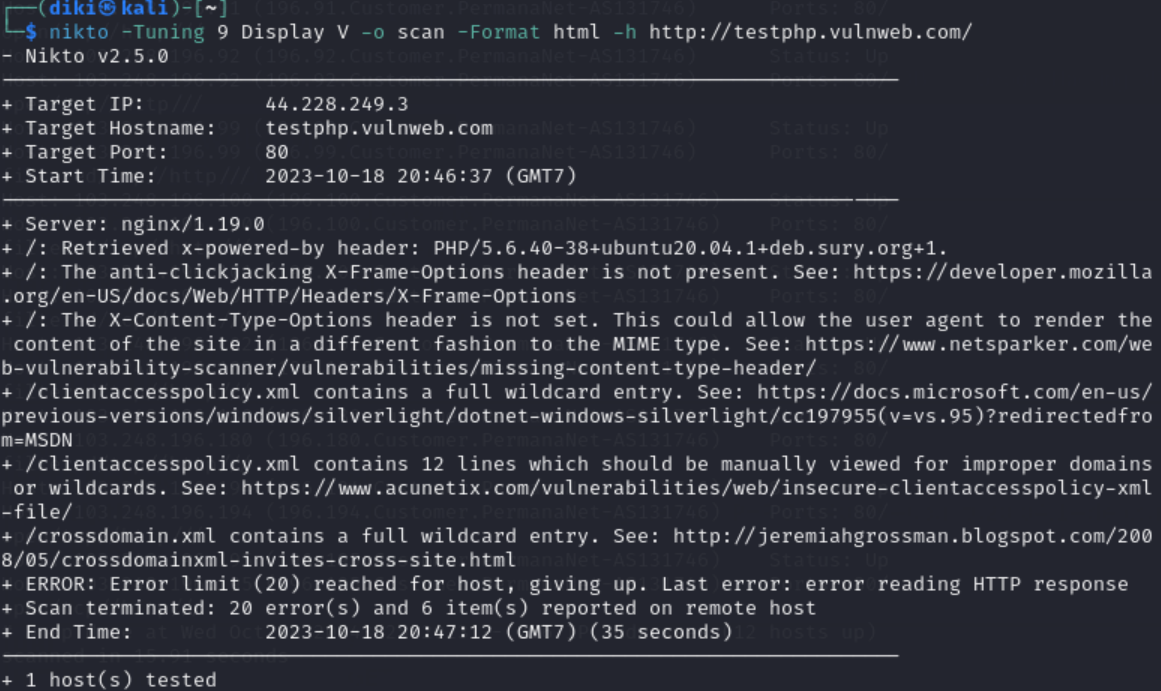


Penjelasan :

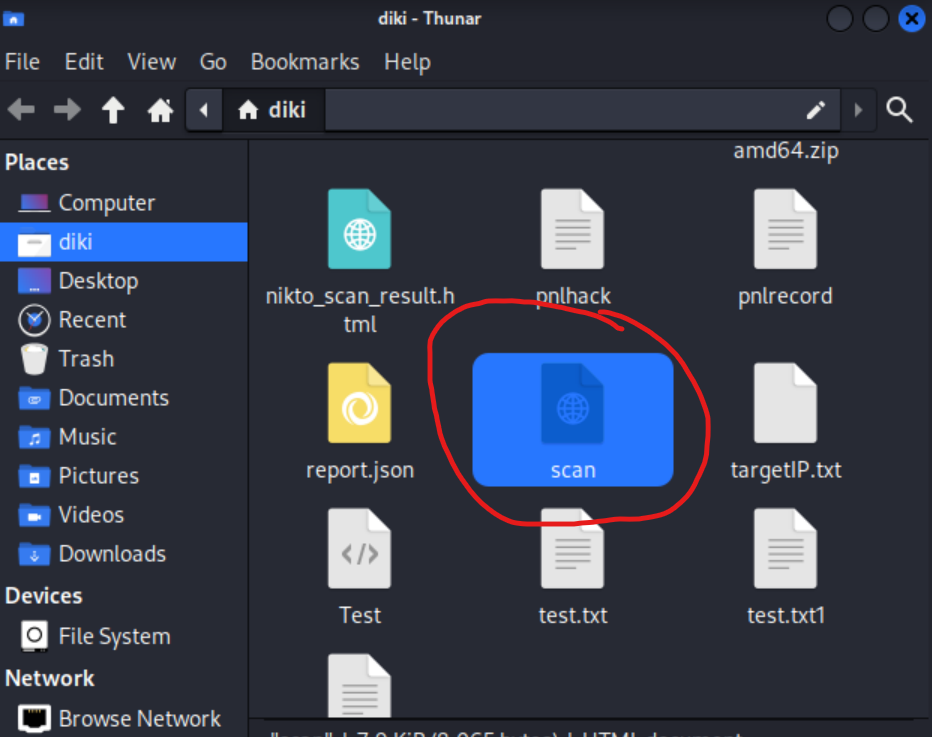
Berikut adalah penjelasan informasi yang diberikan oleh hasil pemindaian:

* **Versi Nikto**: Versi Nikto yang digunakan dalam pemindaian ini adalah v2.5.0.
* **Target IP dan Hostname**: Alamat IP target adalah 44.228.249.3, sementara nama host target adalah "testphp.vulnweb.com."
* **Target Port**: Port yang dituju dalam pemindaian adalah port 80, yang umumnya digunakan untuk layanan web HTTP.
* **Waktu Memulai**: Pemindaian dimulai pada tanggal 18 Oktober 2023 pukul 20:40:19 GMT+7.
* **Server**: Nikto mendeteksi bahwa server yang menjalankan situs web ini adalah "nginx/1.19.0." Informasi ini berguna untuk mengetahui jenis server yang digunakan.
* **Header X-Powered-By**: Pemindaian mengungkap bahwa halaman utama ("/") mengandung header "x-powered-by" yang menyatakan "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1." Ini mengindikasikan bahwa situs web ini menggunakan PHP sebagai bahasa pemrograman server.
* **Header X-Frame-Options**: Pemindaian menyatakan bahwa header "X-Frame-Options" yang digunakan untuk mencegah serangan Clickjacking tidak hadir. Ini adalah kerentanannya yang dapat dieksploitasi jika header ini tidak disetel.
* **Header X-Content-Type-Options**: Pemindaian juga mencatat bahwa header "X-Content-Type-Options" tidak diatur. Ini adalah kerentanan potensial yang dapat memengaruhi cara agen pengguna merender konten situs web.

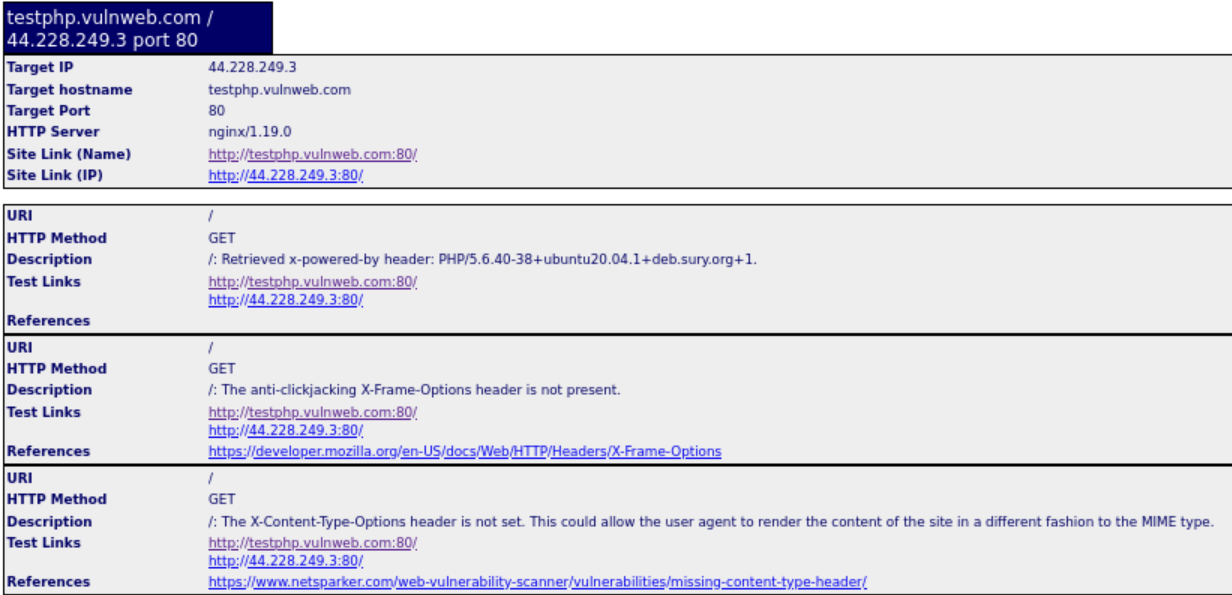
1. Selanjutnya hasil scan nikto akan kita simpan dalam bentuk html dengan perintah $ nikto -Tuning 9 Display V -o scan -Format html -h <http://testphp.vulweb.com/>



Lalu cari di dalam file manager file yang Bernama “scan”



1. Setelah diklik akan muncul seperti berikut ini:



Penjelasannya :

Ini adalah hasil pemindaian yang dilakukan dengan alat Nikto pada situs web "[http://testphp.vulnweb.com](http://testphp.vulnweb.com/)". Berikut adalah sedikit informasi dari hasil pemindaian:

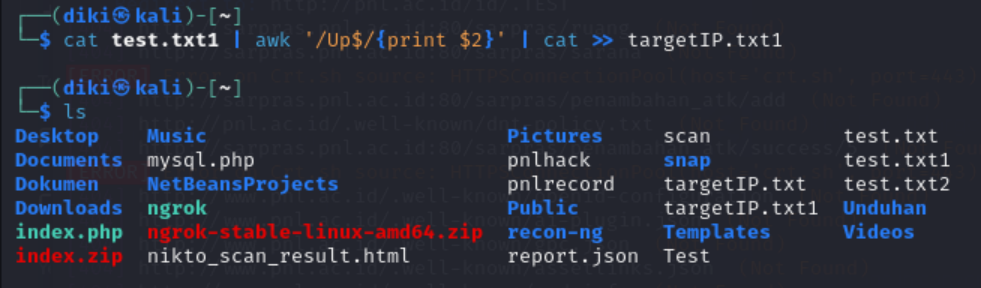
1. **Informasi Target**:
   * Alamat IP Target: 44.228.249.3
   * Hostname Target: testphp.vulnweb.com
   * Port Target: 80
   * Server HTTP: nginx/1.19.0
   * Tautan Situs (Nama): [http://testphp.vulnweb.com:80/](http://testphp.vulnweb.com/)
   * Tautan Situs (IP): [http://44.228.249.3:80/](http://44.228.249.3/)
2. **URI dan Metode HTTP**:
   * URI: /
   * Metode HTTP: GET
   * Deskripsi: Pemindaian mengungkapkan bahwa halaman utama ("/") mengandung header "x-powered-by" yang menyatakan "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1."
3. **Header X-Frame-Options**:
   * URI: /
   * Metode HTTP: GET
   * Deskripsi: Pemindaian menunjukkan bahwa header "X-Frame-Options" yang digunakan untuk mencegah serangan Clickjacking tidak diatur.
4. **Header X-Content-Type-Options**:
   * URI: /
   * Metode HTTP: GET
   * Deskripsi: Pemindaian mencatat bahwa header "X-Content-Type-Options" tidak diatur. Hal ini dapat memungkinkan agen pengguna untuk merender konten situs web dengan cara yang berbeda dari tipe MIME yang seharusnya.
5. **clientaccesspolicy.xml**:
   * URI: /clientaccesspolicy.xml
   * Metode HTTP: GET
   * Deskripsi: clientaccesspolicy.xml berisi entri wildcard lengkap. Referensi diberikan terkait dengan hal ini.
6. **crossdomain.xml**:
   * URI: /crossdomain.xml
   * Metode HTTP: GET
   * Deskripsi: crossdomain.xml berisi entri wildcard lengkap. Referensi juga diberikan terkait dengan ini.

**Ringkasan Pemindaian**:

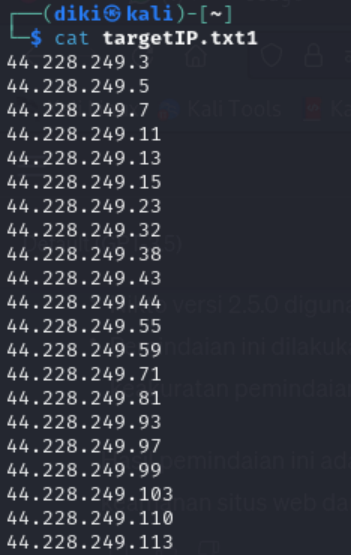
* Pemindaian dilakukan mulai dari pukul 20:46:37 hingga 20:47:12, selama 35 detik.
* Terdapat total 105 permintaan yang dibuat selama pemindaian, dengan 20 kesalahan yang terdeteksi.
* Nikto versi 2.5.0 digunakan dalam pemindaian ini.
* Pemindaian ini dilakukan dengan opsi tuning 9 untuk meningkatkan keakuratan pemindaian.

Hasil pemindaian ini adalah langkah awal yang berguna dalam mengevaluasi keamanan situs web dan mengidentifikasi potensi kerentanannya.

1. Lakukan perintah $ cat test.txt1 | awk '/Up$/{print $2}' | cat >> targetIP.txt1 ini akan mengambil semua IP yang ada pada baris di mana kata "Up" muncul dan menambahkannya ke **targetIP.txt1**. Seluruh baris ini bisa sangat berguna dalam pemrosesan log atau data yang mirip.



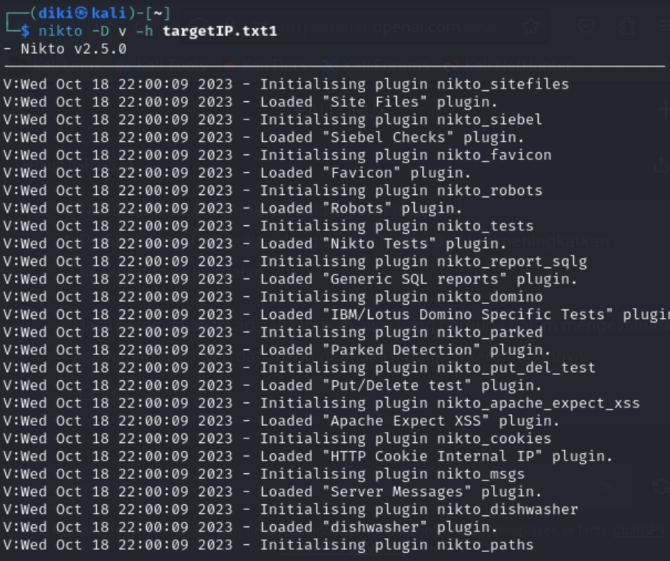
1. Selanjutnya ketik $ cat targetIP.txt1 untuk melihat isi file tersebut.



1. Selanjutnya ketik $ nikto -D v -h targetIP.txt1

Perintah **nikto -D v -h targetIP.txt1** digunakan untuk menjalankan Nikto dengan beberapa opsi tertentu:

* **-D**: Ini digunakan untuk mengaktifkan pemeriksaan database khusus.
* **v**: Ini adalah opsi verbose yang akan menampilkan informasi rinci selama pemindaian.
* **-h targetIP.txt1**: Ini menentukan file target yang akan digunakan oleh Nikto untuk pemindaian.



Penjelasan :

Berikut ini adalah informasi yang terdapat dalam keluaran perintah tersebut:

* Versi Nikto: Nikto versi 2.5.0.
* Daftar plugin yang diinisialisasi dan dimuat, seperti "Site Files," "Siebel Checks," "Favicon," "Robots," "Nikto Tests," dan banyak lagi.
* Daftar target yang akan dipindai, beserta alamat IP dan portnya.
* Informasi tanggal dan waktu inisialisasi pemindaian.