**LAPORAN PRAKTIKUM II**

**INTRO CYBER SECURITY**

****

**NAMA ANGGOTA :**

Diki Candra

Fauzan Maulana

Zia Ulhaq Saputra

Sayed Hadad Bilbina

**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 : 2022903430012

Jurusan : Teknologi Informasi & Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Mata Kuliah : Cyber Scurity

Tanggal Praktikum : 5 Oktober 2023

Tabel Penilaian : :

Mengetahui,

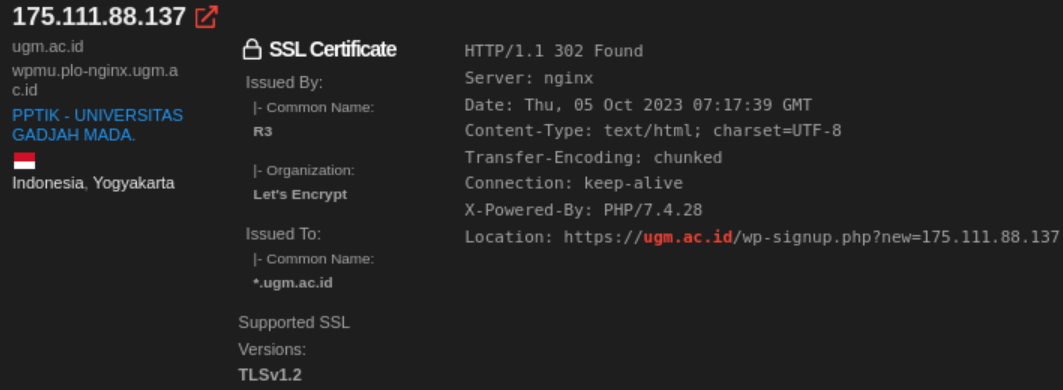
Dosen Pembimbing, Penyusun,

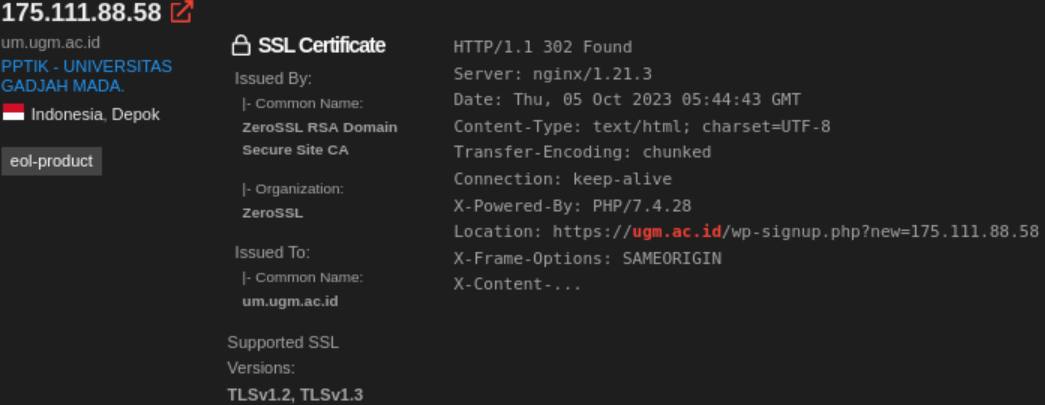
Atthariq, S.ST, MT Diki Candra

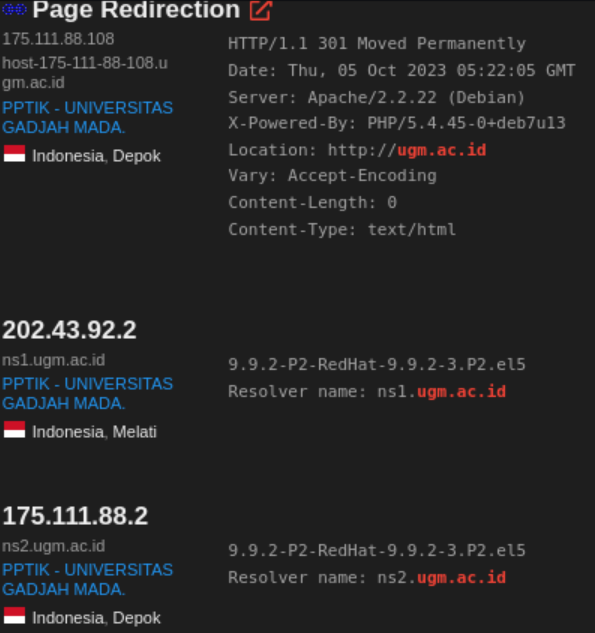
NIP 197807242001121001 NIM 2022903430010

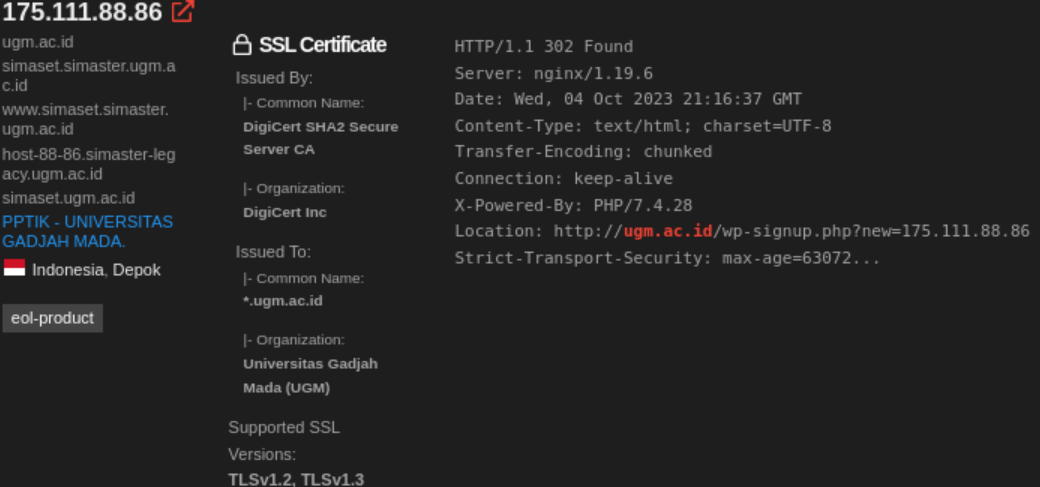
**LANGKAH PERCOBAAN DAN HASIL PERCOBAAN**

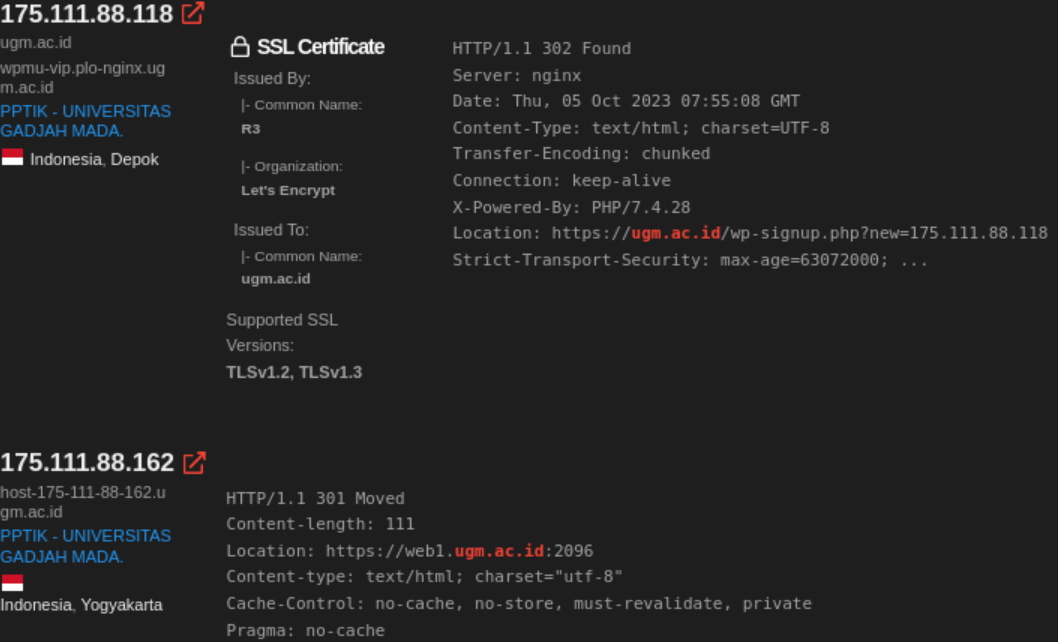
1. Ini adalah shodan, kami menggunakan domain ugm.ac.id

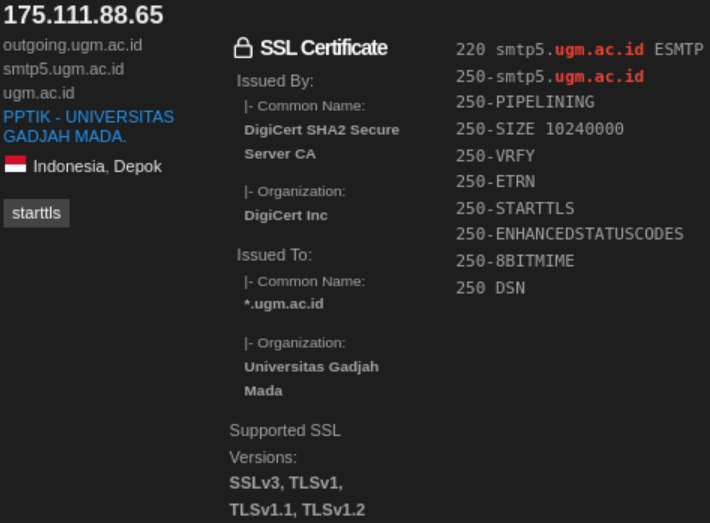


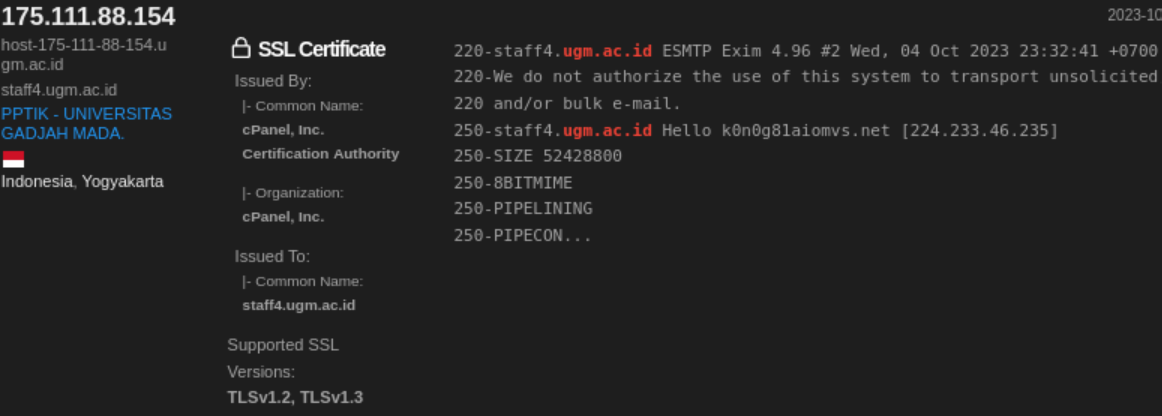




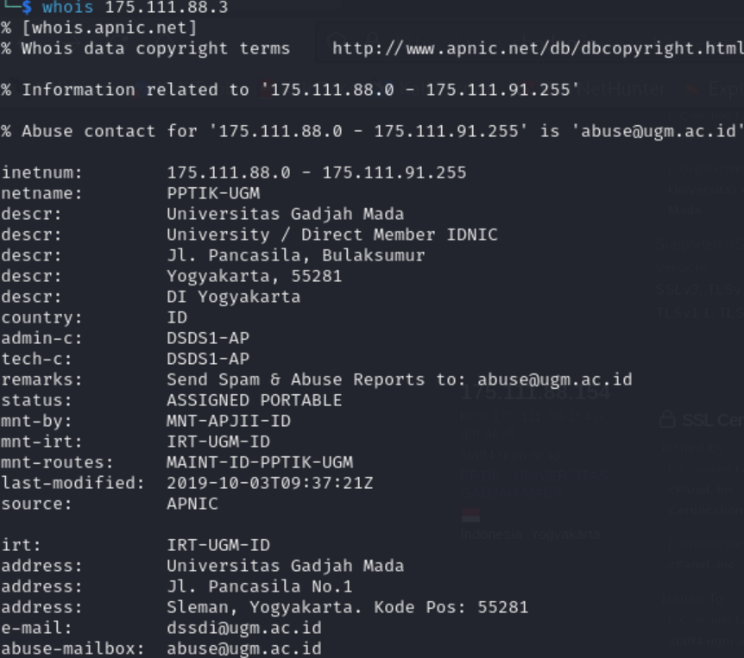


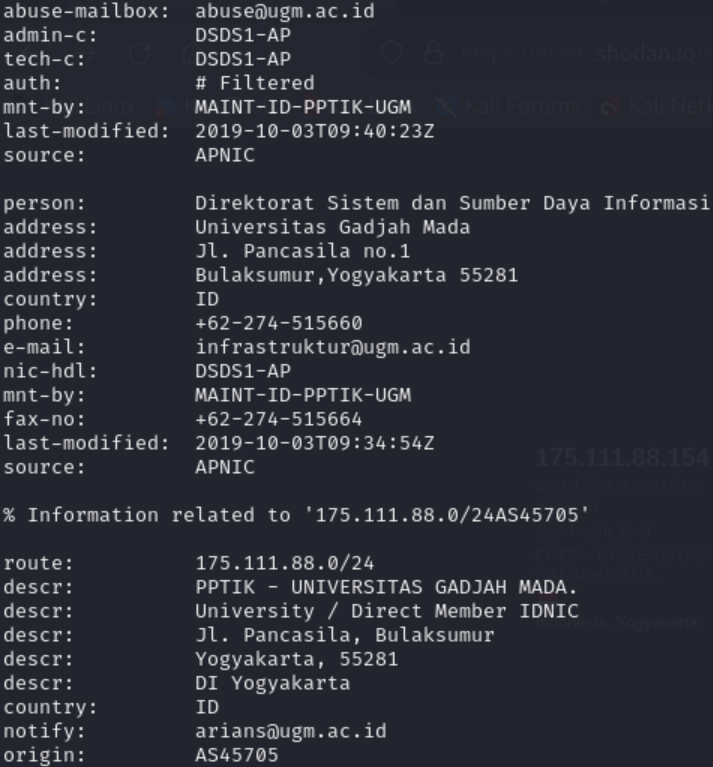






1. Ini whois, kami menggunakan domain ugm.ac.id





**Berikut adalah rangkuman informasi yang terdapat dari praktikum shordan:**

1. 175.111.88.137 (ugm.ac.id)

Lokasi: Yogyakarta, Indonesia

SSL Certificate: Dikeluarkan oleh Let's Encrypt, Common Name: \*.ugm.ac.id

Supported SSL Versions: TLSv1.2

Server: nginx (HTTP/1.1 302 Found)

Redireksi ke <https://ugm.ac.id/wp-signup.php?new=175.111.88.137>

1. 175.111.88.58 (um.ugm.ac.id)

Lokasi: Depok, Indonesia

SSL Certificate: Dikeluarkan oleh ZeroSSL, Common Name: um.ugm.ac.id

Supported SSL Versions: TLSv1.2, TLSv1.3

Server: nginx/1.21.3 (HTTP/1.1 302 Found)

Redireksi ke <https://ugm.ac.id/wp-signup.php?new=175.111.88.58>

1. 175.111.88.108 (host-175-111-88-108.ugm.ac.id)

Lokasi: Depok, Indonesia

Server: Apache/2.2.22 (Debian) (HTTP/1.1 301 Moved Permanently)

Redireksi ke <http://ugm.ac.id>

1. 202.43.92.2 (ns1.ugm.ac.id)

Lokasi: Melati, Indonesia

Resolver name: ns1.ugm.ac.id (BIND version: 9.9.2-P2-RedHat-9.9.2-3.P2.el5)

1. 175.111.88.2 (ns2.ugm.ac.id)

Lokasi: Depok, Indonesia

Resolver name: ns2.ugm.ac.id (BIND version: 9.9.2-P2-RedHat-9.9.2-3.P2.el5)

1. 175.111.88.86 (ugm.ac.id)

Lokasi: Depok, Indonesia

SSL Certificate: Dikeluarkan oleh DigiCert, Common Name: \*.ugm.ac.id

Supported SSL Versions: TLSv1.2, TLSv1.3

Server: nginx/1.19.6 (HTTP/1.1 302 Found)

Redireksi ke <http://ugm.ac.id/wp-signup.php?new=175.111.88.86>

1. 175.111.88.118 (ugm.ac.id)

Lokasi: Depok, Indonesia

SSL Certificate: Dikeluarkan oleh Let's Encrypt, Common Name: ugm.ac.id

Supported SSL Versions: TLSv1.2, TLSv1.3

Server: nginx (HTTP/1.1 302 Found)

Redireksi ke <https://ugm.ac.id/wp-signup.php?new=175.111.88.118>

1. 175.111.88.162 (host-175-111-88-162.ugm.ac.id)

Lokasi: Yogyakarta, Indonesia

Server: (HTTP/1.1 301 Moved)

Redireksi ke <https://web1.ugm.ac.id:2096>

1. 175.111.88.65 (outgoing.ugm.ac.id)

Lokasi: Depok, Indonesia

SSL Certificate: Dikeluarkan oleh DigiCert, Common Name: \*.ugm.ac.id

Supported SSL Versions: SSLv3, TLSv1, TLSv1.1, TLSv1.2

Server: starttls (SMTP)

Pesan: 220 smtp5.ugm.ac.id ESMTP

1. 175.111.88.154 (host-175-111-88-154.ugm.ac.id)

Lokasi: Yogyakarta, Indonesia

SSL Certificate: Dikeluarkan oleh cPanel, Common Name: staff4.ugm.ac.id

Supported SSL Versions: TLSv1.2, TLSv1.3

Server: Exim 4.96 (SMTP)

Pesan: 220-staff4.ugm.ac.id ESMTP Exim 4.96

Informasi ini mencakup lokasi, sertifikat SSL, versi SSL, jenis server, dan pesan HTTP/SMTP terkait setiap alamat IP atau domain yang diidentifikasi. route (175.111.88.0/24AS45705):

**Berikut adalah rangkuman informasi yang terdapat dari praktikum whois:**

1. inetnum (175.111.88.0 - 175.111.91.255):

Netname: PPTIK-UGM

Deskripsi: Universitas Gadjah Mada, Jl. Pancasila, Yogyakarta, ID

Status: ASSIGNED PORTABLE

1. irt (IRT-UGM-ID):

Alamat: Universitas Gadjah Mada, Jl. Pancasila No.1, Sleman, Yogyakarta

Kontak: dssdi@ugm.ac.id, [abuse@ugm.ac.id](mailto:abuse@ugm.ac.id)

1. route (175.111.88.0/24AS45705):

Deskripsi: PPTIK - UNIVERSITAS GADJAH MADA.

Notifikasi: arians@ugm.ac.id

Asal: AS45705

1. inetnum (175.111.88.0 - 175.111.91.255):

Netname: PPTIK-UGM

Deskripsi: PPTIK - UNIVERSITAS GADJAH MADA.

Status: ASSIGNED PORTABLE

1. irt (IRT-IDNIC-ID):

Alamat: Kuningan Barat Gedung Cyber, Jakarta Selatan

Kontak: [abuse@idnic.net](mailto:abuse@idnic.net)

1. person (Direktorat Sistem dan Sumber Daya Informasi):

Alamat: Universitas Gadjah Mada, Jl. Pancasila no.1, Yogyakarta

Kontak: [infrastruktur@ugm.ac.id](mailto:infrastruktur@ugm.ac.id)

route (175.111.88.0/24AS45705):

7. Deskripsi: PPTIK - UNIVERSITAS GADJAH MADA.

Notifikasi: arians@ugm.ac.id

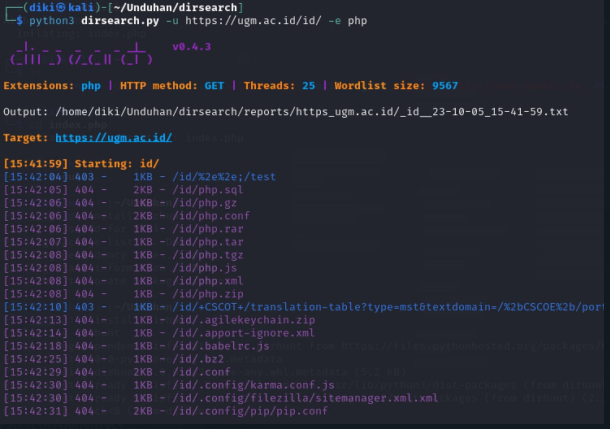
Asal: AS45705

Informasi ini mencakup keterangan IP, informasi jaringan, kontak abuse, dan detail alamat dari entitas yang mengelola alamat IP tersebut.

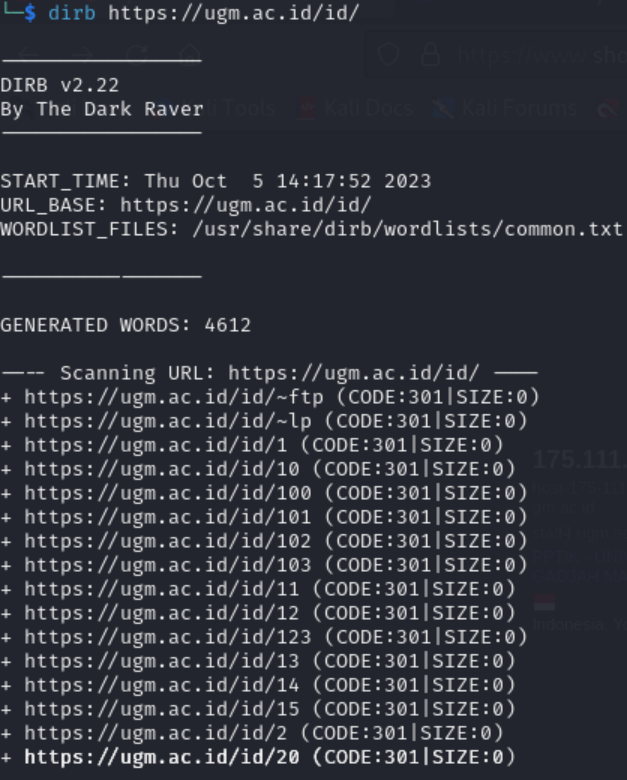
**Perbedaan Shodan dan Whois**

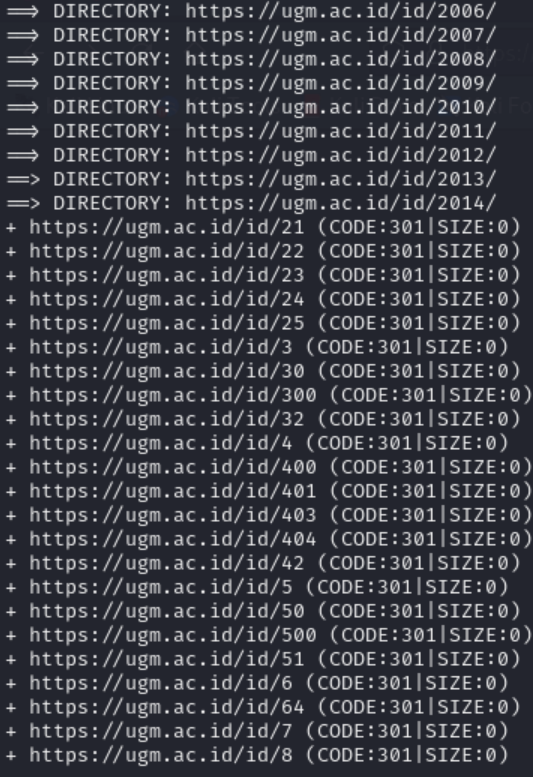
Shodan dan WHOIS pada Kali Linux sebenarnya berperan sebagai alat untuk menganalisis keamanan sistem dan informasi. Shodan seperti mesin pencari yang memungkinkan kita "menggali" perangkat terhubung di internet, sedangkan WHOIS adalah sumber informasi mengenai kepemilikan domain. Jadi, bisa dibilang Shodan membantu menganalisis kerentanan perangkat yang terhubung, sementara WHOIS membantu menganalisis informasi kepemilikan domain.

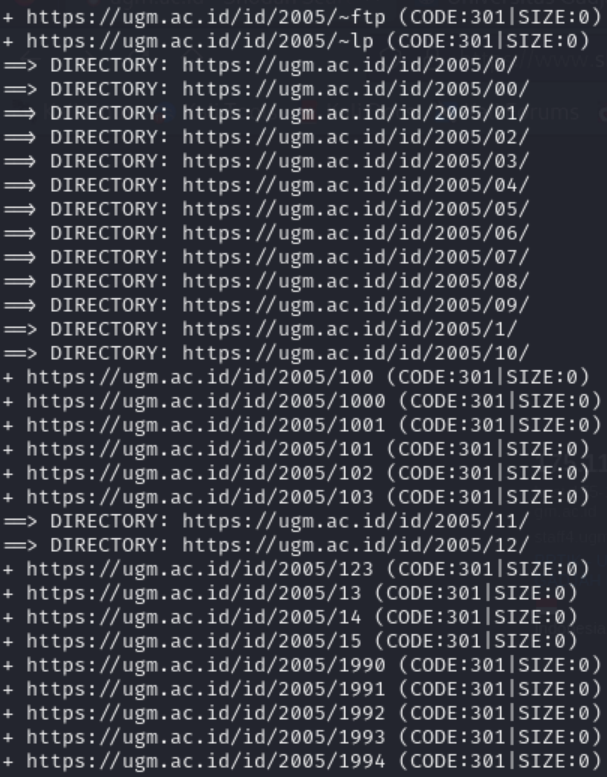
**3. Ini disearch, kami menggunakan domain ugm.ac.id**

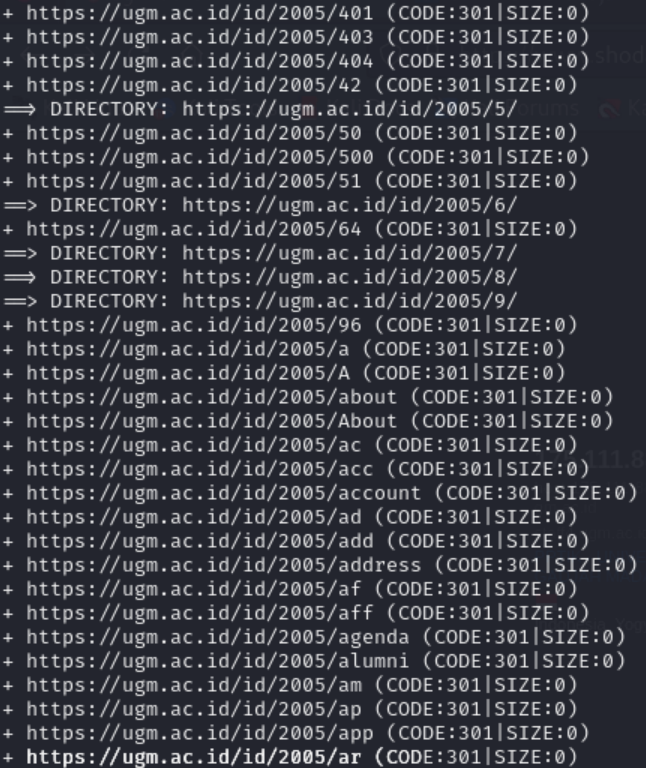


**4. Ini dirbuster, kami menggunakan domain ugm.ac.id**

. 







**Berikut adalah rangkuman informasi yang terdapat dari praktikum dirsearch:**

Informasi yang terdapat adalah 404 Not Found dan 403 Forbidden, Ini adalah kode status yang dikeluarkan oleh server web saat mengelola permintaan clien.

**404 Not Found:**

Kode ini menunjukkan bahwa sumber daya yang diminta oleh klien tidak dapat ditemukan di server. Misalnya, jika Anda mencoba mengakses halaman web yang tidak ada, server akan merespons dengan status 404.

**403 Forbidden:**

Kode ini mengindikasikan bahwa meskipun permintaan dari klien valid, server menolak untuk memberikan respons. Ini sering terjadi ketika klien tidak memiliki izin yang cukup untuk mengakses sumber daya yang diminta.

Dalam konteks Kali Linux, jika Anda melihat kode status ini saat berinteraksi dengan suatu aplikasi web atau server, itu bisa berarti ada masalah dengan sumber daya yang diminta atau ada pembatasan akses yang memerlukan otorisasi yang lebih tinggi.

**Berikut adalah rangkuman informasi yang terdapat dari praktikum dirbuster:**

Informasi yang terdapat adalah HTTP 301. Kode ini mengindikasikan bahwa sumber daya yang diminta oleh klien telah dipindahkan ke lokasi permanen yang berbeda. Oleh karena itu, klien seharusnya mengarahkan permintaan mereka ke lokasi baru yang disediakan dalam respons.

Ini adalah salah satu jenis pengalihan (redirect) yang digunakan dalam web. Pengalihan permanen ini digunakan ketika sumber daya telah dipindahkan secara permanen ke alamat URL yang berbeda. Misalnya, jika sebuah situs web mengubah struktur URL atau pindah ke domain yang berbeda, maka mereka dapat menggunakan kode status 301 untuk memberi tahu klien bahwa mereka harus mengaksesnya di lokasi baru yang diberikan dalam respons.

**Perbedaan Dirsearch dan Dirbuster**

DirBuster adalah alat yang dirancang khusus untuk mengidentifikasi direktori dan file dalam aplikasi web dengan melakukan brute force terhadap nama-nama direktori dan file yang mungkin ada. Ini berfokus pada mencoba banyak kombinasi nama direktori dan file. Sedangkan DirSearch juga digunakan untuk menemukan direktori dan file pada server web, tetapi pendekatannya lebih terstruktur.