LAPORAN TUGAS BESAR – Cyber Security Reconnaissance

Nama: EKO PRASETYO ADI NUGROHO

NIM : 105841114223

Kelas: 5 JK-A

A. Pendahuluan

1. Passive Reconnaissance

Passive Reconnaissance adalah proses pengumpulan informasi terhadap sebuah target tanpa melakukan interaksi langsung dengan sistem target tersebut. Teknik ini hanya memanfaatkan sumber data publik seperti DNS records, historical data, search engine, WHOIS, certificate transparency, dan arsip situs. Karena tidak berinteraksi langsung, metode ini aman, tidak terdeteksi oleh sistem keamanan target, serta banyak digunakan dalam tahap awal penetration testing.

Beberapa jenis informasi yang biasanya dikumpulkan pada passive recon antara lain:

- Identitas domain (WHOIS)
- Informasi DNS dan subdomain
- Server dan teknologi yang digunakan
- Riwayat versi situs (Wayback Machine)
- Informasi email publik perusahaan
- Informasi port/IP dari sumber publik
- File sensitif yang pernah terekspos di internet

Tujuan utama passive recon adalah membangun profil lengkap target sebelum melakukan teknik yang lebih intrusif.

2. Active Reconnaissance

Active Reconnaissance adalah proses pengumpulan informasi dengan cara melakukan interaksi langsung dengan sistem target, seperti scanning port, probing service, enumerasi sistem, dan eksploitasi terhadap kerentanan. Metode ini memiliki risiko tinggi karena dapat terdeteksi oleh firewall, IDS/IPS, dan log server.

Active recon biasanya dilakukan pada lingkungan lab atau sistem yang memang disediakan untuk tujuan pembelajaran, seperti VulnOS atau Metasploitable.

Informasi yang dikumpulkan melalui active recon antara lain:

a. Port dan service yang terbuka
b. Versi layanan
c. Sistem operasi target
d. Kerentanan yang dapat dieksploitasi
e. Akses shell (bila eksploitasi berhasil)

3. Tujuan Tugas Besar

Tugas ini bertujuan untuk memberikan pemahaman mengenai:

a. Perbedaan dan implementasi Passive Recon dan Active Recon dalam proses penetration testing.
b. Melatih kemampuan melakukan pengumpulan informasi terhadap target nyata (web industri/E-commerce/pemerintahan) dengan teknik yang etis dan legal.
c. Mengimplementasikan active recon pada sistem rentan (VulnOS / Metasploitable 3) untuk mempraktikkan scanning, enumerasi, serta eksploitasi.

d. Membangun dokumentasi lengkap berupa screenshot, laporan, dan skenario penggunaan tools.

e. Membuat repositori GitHub sebagai pusat penyimpanan seluruh berkas tugas (skenario, dokumentasi, laporan).

f. Membuat video dokumentasi dan publikasi ke YouTube sebagai bentuk presentasi praktikum.

Dengan tujuan ini diharapkan peserta mampu memahami proses pentesting secara menyeluruh dari tahap persiapan, rekonstruksi informasi, hingga penyusunan laporan akhir.

4. Tools yang Digunakan

Berikut daftar tools utama yang digunakan dalam tugas besar:

Tools Passive Recon:

a. WHOIS Lookup

b. Dig

c. Subfinder

d. Amass (Passive Mode)

e. crt.sh

f. Censys

g. Wappalyzer

h. Wayback Machine

i. robots.txt

j. sitemap.xml

k. HTTP Header Checking (curl -I)

B. Skenario Tugas Besar

1. PASSIVE RECON

Target

1. **Domain:** growtopiagame.com
2. **Industri:** Game online / gaming server
3. **Tujuan:** Mengumpulkan informasi sebanyak mungkin tanpa melakukan interaksi langsung (non-intrusive) terhadap server target.

a. Tahap 1 – Identifikasi Informasi Domain

1. Perintah

whois growtopiagame.com

2. Data yang Dicari untuk Laporan

- Registrar
- Creation date
- Name Server
- Organization

b. Tahap 2 – DNS Enumeration

dig digunakan untuk melihat record DNS domain secara pasif (tidak menyerang, hanya meminta informasi publik).

Tujuannya untuk mengetahui:

1. *A record (alamat IP utama)*
2. *MX (mail server)*
3. *NS (nameserver)*

4. *TXT records (kadang berisi konfigurasi penting)*

c. Tahap 3 – Enumerasi Subdomain

1. Perintah

subfinder -d growtopiagame.com

amass enum -passive -d growtopiagame.com

2. Tujuan

- Mengumpulkan subdomain publik
- Menggabungkan hasil dari dua tools pasif
- Menemukan potensi attack surface

d. Tahap 4 – SSL Certificate Analysis (crt.sh)

1. URL

https://crt.sh/?q=growtopiagame.com

2. Yang Dikumpulkan

- Subdomain dari certificate transparency logs
- Issuer Certificate
- Validity date

e. Tahap 5 – Passive Scan via Censys

1. Query

growtopiagame.com

2. Yang Dicari & Screenshot

- daftar host ditemukan
- protokol layanan (HTTP, HTTPS, TCP ports, dll.)

- semua port terbuka
- ASN
- lokasi server

f. Tahap 6 – Identifikasi Teknologi Web

Menggunakan **Wappalyzer (Browser Extension)**

1. **Yang Dicari**
   - Web Server (nginx, Apache, Cloudflare, dsb.)
   - Framework / CMS
   - CDN
   - Analytics
   - Security headers

g. Tahap 7 – Arsip Situs via Wayback Machine

1. **URL**

   https://web.archive.org/web/*/growtopiagame.com

2. **Yang Dicari**
   - Timeline snapshot
   - Perubahan konten
   - Potensi endpoint lama

h. **Tahap 8 – File Publik (Passive Discovery)**

1. **robots.txt**

   curl -s https://growtopiagame.com/robots.txt

2. **sitemap.xml**

   curl -s https://growtopiagame.com/sitemap.xml

3. **Header HTTP**

   curl -I https://growtopiagame.com

4. **Google Dorking, Github Gorking**

   site:github.com "growtopiagame.com" password

   site:github.com "growtopiagame.com" config

5. **Tujuan**

   - Mengetahui path publik
   - Struktur website
   - Security header seperti HSTS, CSP, X-Frame-Options, dll.
   - Menegtahui hal sensitive yang tidak sengaja terindeks

i. **Tahap 9 - Identifikasi Karyawan & Kontak (OSINT)**

1. **URL**

   https://rocketreach.co

2. **Tujuan**

   - Mengetahui nama karyawan beserta jabatan dan emailnya

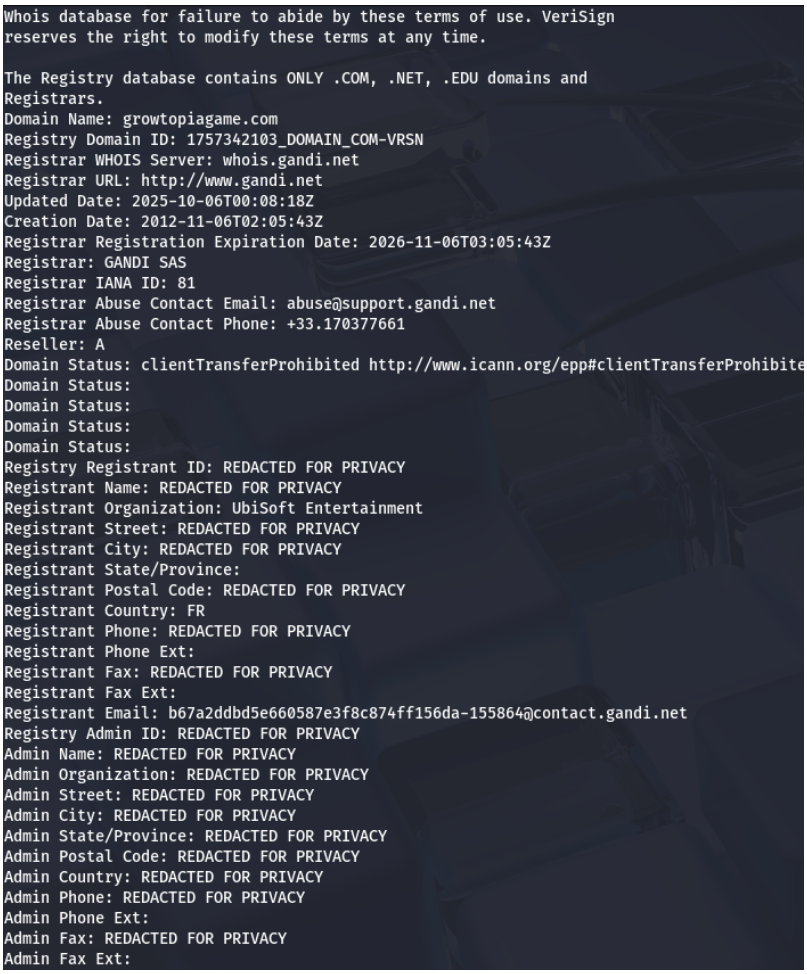
2. **Active Recon**

- Target: **VulnOS**
- Tujuan: Mengidentifikasi layanan dan potensi kerentanan

C. Passive Recon – Dokumentasi Langkah per Langkah

1. Whois Lookup


```
┌──(newbie㉿kali)-[~]
└─$ whois growtopiagame.com

   Domain Name: GROWTOPIAGAME.COM
   Registry Domain ID: 1757342103_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gandi.net
   Registrar URL: http://www.gandi.net
   Updated Date: 2025-10-06T00:08:18Z
   Creation Date: 2012-11-06T03:05:43Z
   Registry Expiry Date: 2026-11-06T03:05:43Z
   Registrar: Gandi SAS
   Registrar IANA ID: 81
   Registrar Abuse Contact Email: abuse@support.gandi.net
   Registrar Abuse Contact Phone: +33.170377661
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NIC10.UBISOFT.COM
   Name Server: NIC11.UBISOFT.COM
   Name Server: NIC12.UBISOFT.COM
   Name Server: NIC7.UBISOFT.COM
   Name Server: NIC8.UBISOFT.COM
   Name Server: NIC9.UBISOFT.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-08T13:25:53Z <<<
```



NARASI

Pada tahap ini, dilakukan eksekusi perintah whois growtopiagame.com melalui terminal. Kode perintah ini berfungsi untuk mengirimkan permintaan (*query*) ke basis data publik WHOIS yang menyimpan catatan pendaftaran domain di internet. Tujuannya adalah untuk melakukan pengumpulan informasi awal (*information gathering*) guna mengetahui identitas pemilik domain, penyedia layanan pendaftaran (registrar), serta infrastruktur dasar yang digunakan oleh target tanpa harus berinteraksi langsung dengan sistem mereka.

Hasil dari eksekusi kode tersebut menampilkan data administratif lengkap terkait domain growtopiagame.com. Dari output yang dihasilkan, teridentifikasi bahwa domain ini terdaftar melalui registrar **Gandi SAS** dan secara resmi dimiliki oleh organisasi **Ubisoft Entertainment**, yang dibuktikan dengan penggunaan *Name Server* (NS) yang mengarah ke server Ubisoft. Selain itu, data tersebut juga memperlihatkan bahwa domain ini telah aktif sejak tahun 2012 dengan masa berlaku hingga tahun 2026 dan *Registran Countrynya* ialah Prancis, meskipun detail kontak personal administrator disembunyikan (*redacted*) untuk alasan perlindungan privasi data.

2. DNS Enumeration

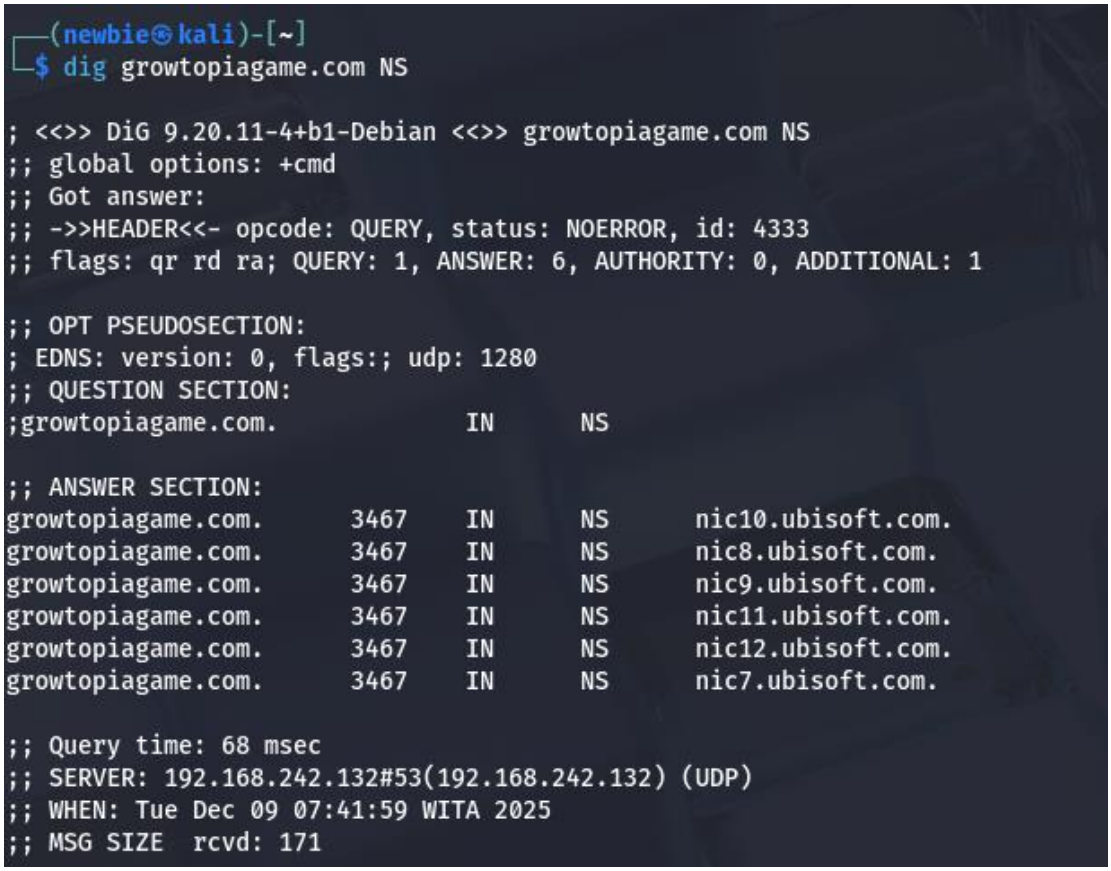
a. Analisis Record A (Address)

```
┌──(newbie㉿kali)-[~]
└─$ dig growtopiagame.com A

; <<>> DiG 9.20.11-4+b1-Debian <<>> growtopiagame.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25618
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;growtopiagame.com.             IN      A

;; ANSWER SECTION:
growtopiagame.com.      20      IN      A       3.234.190.161
growtopiagame.com.      20      IN      A       34.237.104.171

;; Query time: 172 msec
;; SERVER: 192.168.242.132#53(192.168.242.132) (UDP)
;; WHEN: Tue Dec 09 07:40:13 WITA 2025
;; MSG SIZE  rcvd: 78
```

NARASI

menjalankan perintah dig growtopiagame.com A untuk melakukan pencarian DNS record tipe A. Perintah ini berfungsi memetakan nama domain ke alamat IP (IPv4) agar dapat mengetahui lokasi server hosting secara spesifik. Dari hasil eksekusi (pada bagian *Answer Section*), ditemukan bahwa domain tersebut mengarah ke dua alamat IP publik, yaitu 3.234.190.161 dan 34.237.104.171. Penemuan dua IP ini mengindikasikan adanya penggunaan mekanisme *load balancing* atau redundansi untuk menjaga ketersediaan layanan *game* tersebut.

b. Analisis Record NS (Name Server)



NARASI

perintah dig growtopiagame.com NS untuk mengidentifikasi *Name Server* otoritatif yang menangani zona DNS domain ini. Kode ini bertujuan mengetahui infrastruktur DNS yang digunakan oleh target. Hasil output menunjukkan daftar server DNS yang digunakan sangat banyak dan semuanya berakhiran .ubisoft.com (seperti nic10.ubisoft.com, nic8.ubisoft.com, dst). Hal ini mengonfirmasi secara teknis bahwa infrastruktur jaringan dan manajemen domain growtopiagame.com dikelola penuh secara internal oleh perusahaan induknya, yaitu Ubisoft.

c. Analisis Record MX (Mail Exchange)

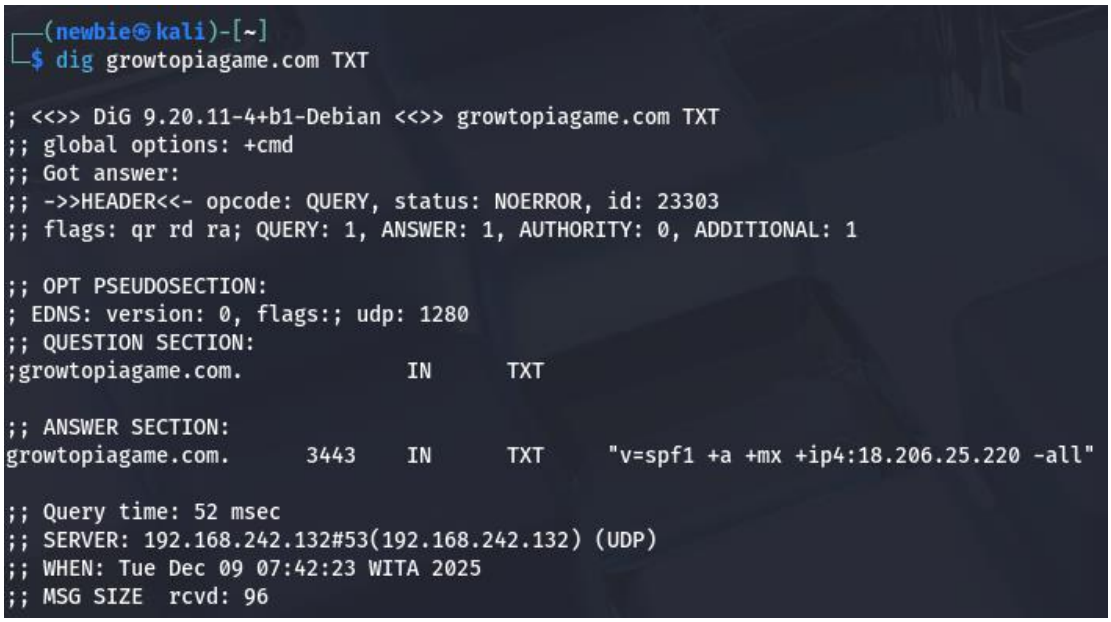
```
┌──(newbie㉿kali)-[~]
└─$ dig growtopiagame.com MX

; <<>> DiG 9.20.11-4+b1-Debian <<>> growtopiagame.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50502
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;growtopiagame.com.             IN      MX

;; ANSWER SECTION:
growtopiagame.com.      3490    IN      MX      10 mail1.growtopiagame.com.

;; ADDITIONAL SECTION:
mail1.growtopiagame.com. 3490   IN      A       18.206.25.220

;; Query time: 172 msec
;; SERVER: 192.168.242.132#53(192.168.242.132) (UDP)
;; WHEN: Tue Dec 09 07:41:35 WITA 2025
;; MSG SIZE  rcvd: 84
```

NARASI

perintah dig growtopiagame.com MX. Perintah ini digunakan untuk mencari *Mail Exchange record*, yang memberi tahu server lain ke mana harus mengirimkan email

yang ditujukan untuk domain ini. Hasilnya menunjukkan bahwa domain ini menggunakan mail server mail1.growtopiagame.com dengan prioritas 10. Selain itu, pada bagian *Additional Section*, sistem secara otomatis melakukan resolusi nama mail server tersebut ke alamat IP **18.206.25.220**, yang berarti server emailnya terpisah dari server web utamanya.

Analisis Record TXT (Text/SPF)



NARASI

perintah dig growtopiagame.com TXT untuk mengambil catatan teks yang tertanam pada DNS. Seringkali, record ini berisi kebijakan keamanan seperti SPF (*Sender Policy Framework*). Hasil output menampilkan data string "v=spf1 +a +mx +ip4:18.206.25.220 -all". Data ini merupakan konfigurasi keamanan email yang mendefinisikan siapa saja yang diizinkan mengirim email atas nama domain ini. Berdasarkan output tersebut, hanya IP server web (record A), mail server (record MX), dan IP spesifik 18.206.25.220 yang sah untuk mengirim email, sedangkan sumber lain akan ditolak (*-all*).

3. **Subdomain Enumeration**

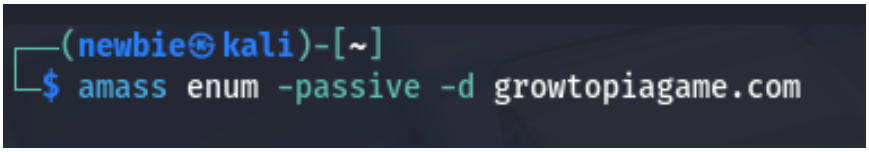
   a. **Subfinder: Pencarian Cepat (Discovery)**

NARASI

dilakukan pencarian cepat menggunakan perintah subfinder -d growtopiagame.com. Alat ini bekerja dengan mengumpulkan data dari sumber pasif publik. Hasil eksekusinya berhasil menemukan sejumlah subdomain krusial seperti login.growtopiagame.com (portal akses), backup.growtopiagame.com (potensi data cadangan), host01.growtopiagame.com, serta xsolla.growtopiagame.com yang mengindikasikan adanya sistem pembayaran eksternal. Penemuan subdomain seperti

beta dan backup sangat bernilai karena sering kali memiliki celah keamanan yang tidak sebaik domain utama.

b. OWASP Amass: Pemetaan Infrastruktur (Mapping)

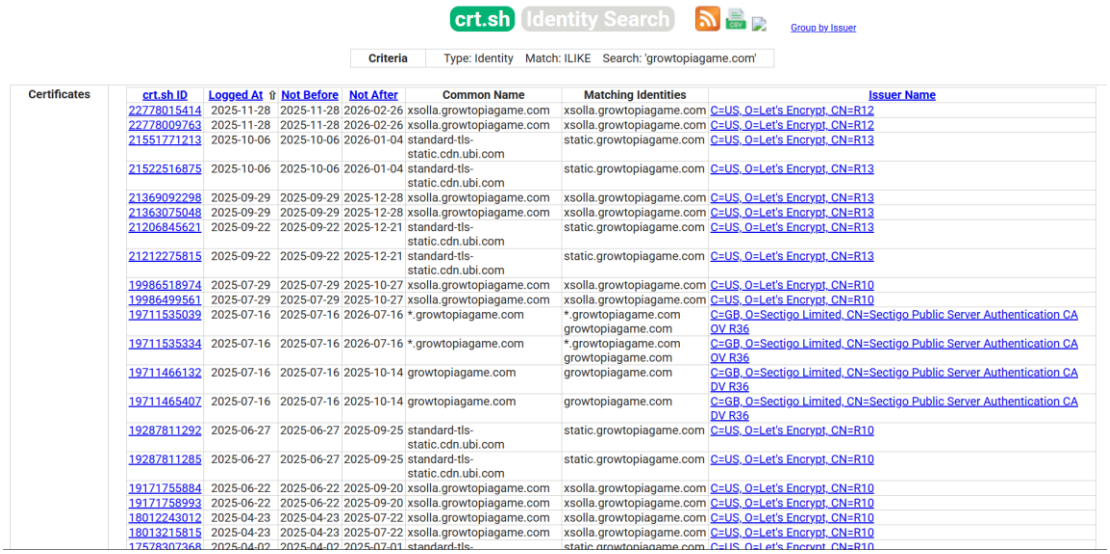



```
growtopiagame.com (FQDN) --> a_record --> 18.206.109.172 (IPAddress)
growtopiagame.com (FQDN) --> a_record --> 54.158.187.82 (IPAddress)
cdn.growtopiagame.com (FQDN) --> cname_record --> cdn.growtopiagame.com.s3-eu-west-1.amazonaws.com (FQDN)
18.204.0.0/14 (Netblock) --> contains --> 18.206.109.172 (IPAddress)
54.156.0.0/14 (Netblock) --> contains --> 54.158.187.82 (IPAddress)
14618 (ASN) --> managed_by --> AMAZON-AES - Amazon.com, Inc. (RIROrganization)
14618 (ASN) --> announces --> 18.204.0.0/14 (Netblock)
14618 (ASN) --> announces --> 54.156.0.0/14 (Netblock)
```

NARASI

untuk mendapatkan pemetaan infrastruktur yang lebih komprehensif, digunakan perintah amass enum -passive -d growtopiagame.com. Berbeda dengan sebelumnya, alat ini tidak hanya mencari nama subdomain, tetapi juga memetakan hubungan infrastrukturnya. Dari output yang dihasilkan, terlihat bahwa subdomain cdn.growtopiagame.com diarahkan ke layanan *cloud storage* Amazon S3, dan infrastruktur jaringan target teridentifikasi menggunakan ASN 14618 milik **Amazon.com, Inc.**. Informasi ini mengonfirmasi bahwa target sangat bergantung pada layanan *cloud* AWS (Amazon Web Services) untuk operasional backend-nya.

4. crt.sh Certificate Lookup



crt.sh Identity Search Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'growtopiagame.com'

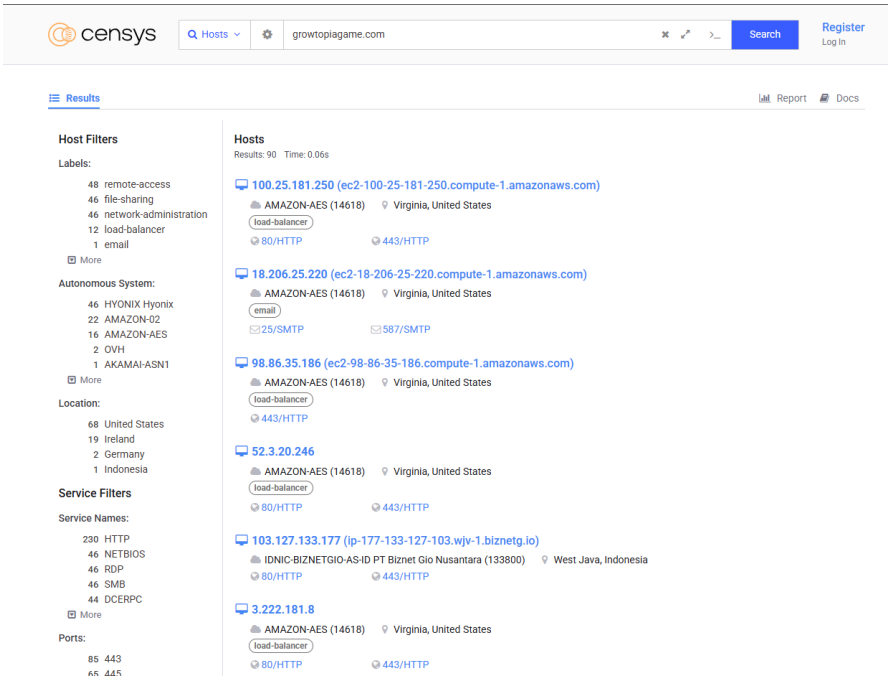
Certificates

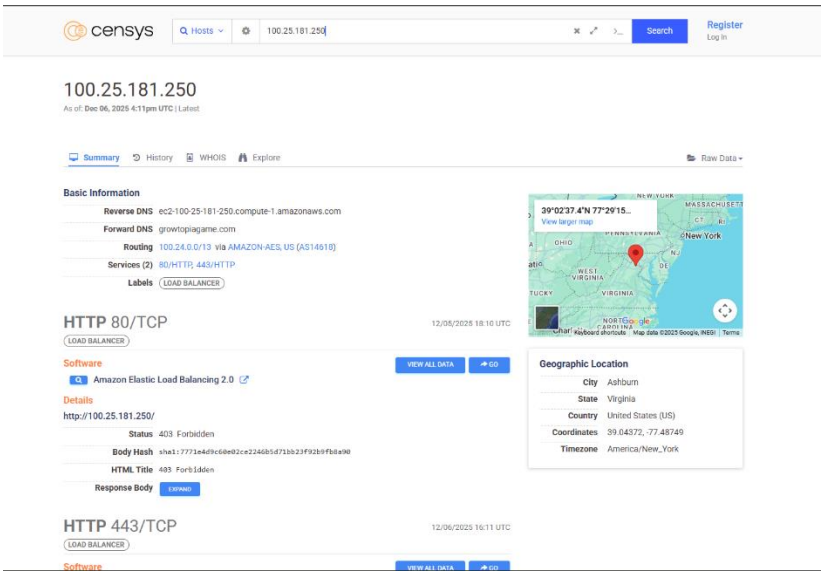
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
22778015414	2025-11-28	2025-11-28	2026-02-26	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R12
22778009763	2025-11-28	2025-11-28	2026-02-26	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R12
21551771213	2025-10-06	2025-10-06	2026-01-04	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
21522516875	2025-10-06	2025-10-06	2026-01-04	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
21369092298	2025-09-29	2025-09-29	2025-12-28	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
21363075048	2025-09-29	2025-09-29	2025-12-28	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
21206845621	2025-09-22	2025-09-22	2025-12-21	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
21212275815	2025-09-22	2025-09-22	2025-12-21	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R13
19986518974	2025-07-29	2025-07-29	2025-10-27	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
19986499561	2025-07-29	2025-07-29	2025-10-27	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
19711535039	2025-07-16	2025-07-16	2026-07-16	*.growtopiagame.com	*.growtopiagame.com growtopiagame.com	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA OV R36
19711535334	2025-07-16	2025-07-16	2026-07-16	*.growtopiagame.com	*.growtopiagame.com growtopiagame.com	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA OV R36
19711466132	2025-07-16	2025-07-16	2025-10-14	growtopiagame.com	growtopiagame.com	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
19711465407	2025-07-16	2025-07-16	2025-10-14	growtopiagame.com	growtopiagame.com	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
19287811292	2025-06-27	2025-06-27	2025-09-25	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
19287811285	2025-06-27	2025-06-27	2025-09-25	standard-tls-static.cdn.ubi.com	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
19171755884	2025-06-22	2025-06-22	2025-09-20	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
19171758993	2025-06-22	2025-06-22	2025-09-20	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
18012243012	2025-04-23	2025-04-23	2025-07-22	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
18013215815	2025-04-23	2025-04-23	2025-07-22	xsolla.growtopiagame.com	xsolla.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10
17578307368	2025-04-02	2025-04-02	2025-07-01	standard-tls-	static.growtopiagame.com	C=US, O=Let's Encrypt, CN=R10

NARASI

Selain menggunakan terminal, dilakukan juga teknik *Passive Reconnaissance* menggunakan layanan web crt.sh. Langkah ini bertujuan untuk mencari jejak digital domain melalui log *Certificate Transparency* yang merekam riwayat penerbitan sertifikat SSL/TLS. Dari hasil pencarian ini, ditemukan berbagai subdomain yang mungkin tidak terpublikasi secara umum, seperti xsolla.growtopiagame.com (kemungkinan untuk pembayaran), login.growtopiagame.com (portal masuk), dan static.growtopiagame.com (aset statis). Hasil ini juga memperlihatkan penggunaan otoritas sertifikat seperti *Let's Encrypt* dan *Sectigo Limited* dalam mengamankan komunikasi data mereka.

5. Pemindaian Infrastruktur & Layanan (Censys)





NARASI

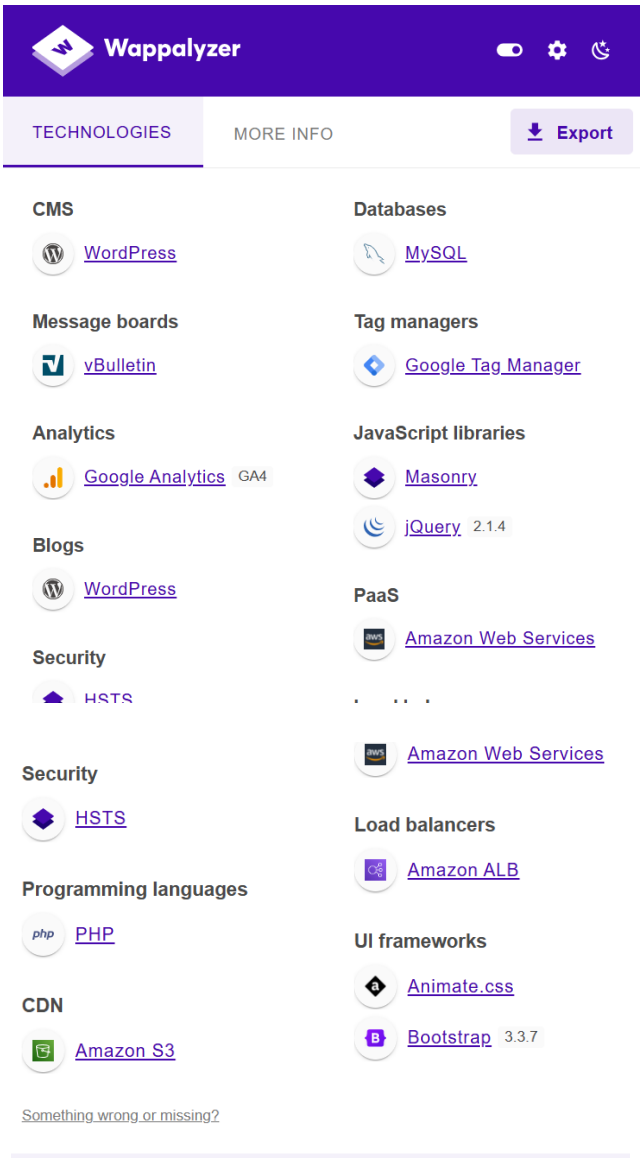
Dengan menggunakan mesin pencari **Censys** untuk memetakan perangkat dan layanan yang terhubung ke internet yang diasosiasikan dengan domain growtopiagame.com.

Berbeda dengan pencarian DNS, Censys memindai alamat IP dan *port* untuk mengidentifikasi perangkat lunak server, lokasi fisik, dan penyedia layanan *hosting*.

Hasil pencarian awal menunjukkan bahwa infrastruktur *game* ini tersebar di berbagai penyedia layanan, terutama **Amazon Web Services (AWS)** di wilayah Virginia, AS, serta beberapa server di **OVH** (Jerman) dan **I3DNET**. Teridentifikasi berbagai *port* terbuka seperti 80 (HTTP), 443 (HTTPS), dan port manajemen seperti 22 (SSH) dan 3389 (RDP) pada beberapa host tertentu, yang bisa menjadi titik masuk potensial jika tidak diamankan dengan baik.

Pemeriksaan lebih mendalam dilakukan terhadap salah satu *host* kunci dengan IP **100.25.181.250**. Detail host ini mengonfirmasi penggunaannya sebagai **Amazon Elastic Load Balancing 2.0**, yang bertugas mendistribusikan trafik pengguna. Dari sisi keamanan aplikasi, server merespons dengan kode **403 Forbidden** saat diakses langsung melalui IP, menandakan konfigurasi keamanan yang baik karena mencegah akses langsung tanpa nama domain yang valid. Analisis pada sertifikat TLS/SSL host ini juga memvalidasi kepemilikan sah, dengan subjek sertifikat tertulis **O=Ubisoft Divertissements Inc.** dan diterbitkan oleh **Sectigo Limited**, yang membuktikan bahwa server ini adalah aset resmi milik pengembang *game* tersebut.

6. Identifikasi Teknologi Web

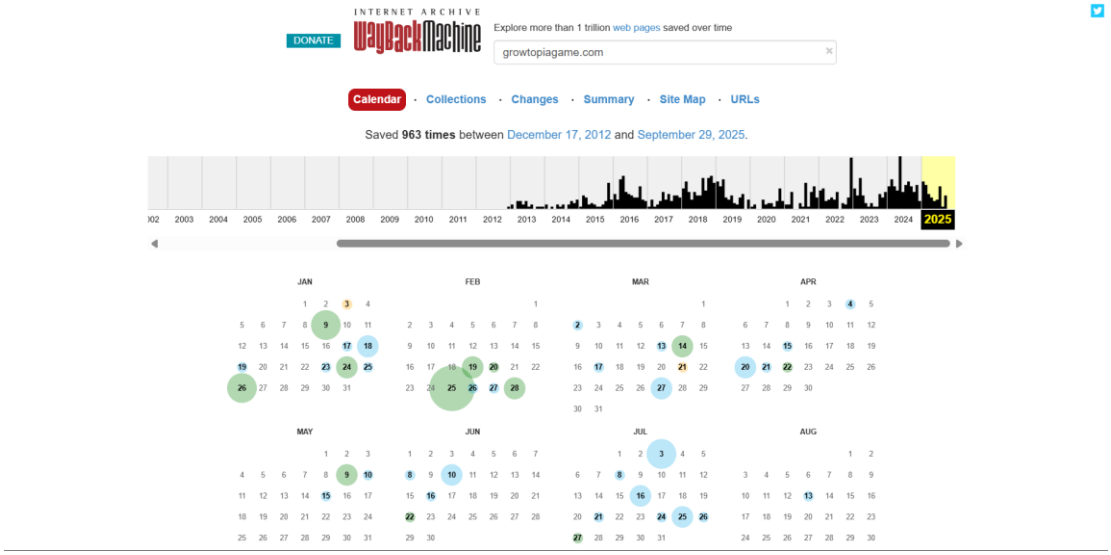


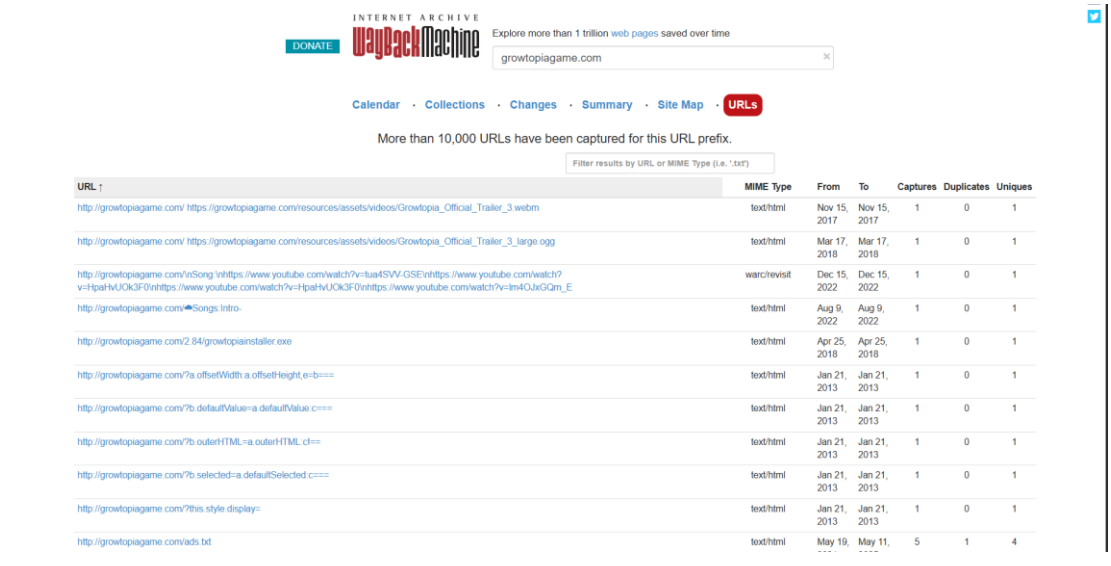
NARASI

Berdasarkan analisis menggunakan **Wappalyzer**, diketahui bahwa situs growtopiagame.com dibangun di atas fondasi **PHP** dan database **MySQL**, dengan menggunakan **WordPress** sebagai CMS utama serta **vBulletin** untuk layanan forum

komunitasnya. Seluruh infrastruktur situs ini dikelola menggunakan layanan **Amazon Web Services (AWS)**, yang mencakup **Amazon S3** untuk penyimpanan aset (*CDN*) dan **Amazon ALB** untuk menyeimbangkan beban trafik server. Untuk tampilan antarmuka, situs ini mengandalkan *framework* **Bootstrap 3.3.7** dan pustaka **jQuery** agar responsif dan interaktif.

7. Wayback Machine





NARASI

Untuk melacak jejak digital masa lalu, digunakan layanan **Wayback Machine** dari Internet Archive. Alat ini berhasil mengidentifikasi **963 rekaman (snapshot)** halaman web growtopiagame.com yang tersimpan sejak Desember 2012 hingga 2025. Melalui arsip ini, ditemukan akses ke aset-aset lama yang mungkin sudah dihapus dari situs aktif saat ini, seperti file instalasi lawas (growtopiainstaller.exe) dan materi promosi video lama, yang berguna untuk menganalisis perubahan konten target dari waktu ke waktu

8. **Pemeriksaan File Publik & Keamanan HTTP.**
   a. **Analisis Kebijakan Crawler (robots.txt)**

NARASI

Pemeriksaan dimulai dengan mengecek file robots.txt menggunakan perintah curl. File ini berisi instruksi bagi *search engine* mengenai direktori mana yang tidak boleh diindeks. Dari hasil *output*, ditemukan beberapa jalur sensitif yang disembunyikan (*Disallow*), seperti /forums/admincp/, /forums/usage/, dan /vanguard/. Penemuan direktori /admincp/ sangat krusial karena mengindikasikan lokasi halaman login administrator forum yang bisa menjadi target serangan potensial

b. Pemeriksaan Struktur Situs (sitemap.xml)

```
┌──(newbie㉿kali)-[~]
└─$ curl -s https://growtopiagame.com/sitemap.xml
<!DOCTYPE html>
<html>
    <head>
        <title>Growtopia Game - Page not found [404]</title>
        <link rel="icon" type="image/png" href="https://s3.eu-west-1.amazonaws.com/cdn.growtopiagame.com/website/resources/assets/images/growtopia.ico" sizes="16x16" />
                <link rel="shortcut icon" href="https://s3.eu-west-1.amazonaws.com/cdn.growtopiagame.com/website/resources/assets/images/growtopia.ico" type="image/x-icon">
                <link rel="icon" href="https://s3.eu-west-1.amazonaws.com/cdn.growtopiagame.com/website/resources/assets/images/growtopia.ico" type="image/x-icon">
                <link media="all" rel="stylesheet" href="https://s3.eu-west-1.amazonaws.com/cdn.growtopiagame.com/website/resources/assets/css/custom.css">
        <style>
            html, body {
                height: 100%;
            }

            body {
                margin: 0;
                padding: 0;
                width: 100%;
                display: table;
                /* The image used */
                font-family: CenturyGothicBold;
                            background-image: url( https://s3.eu-west-1.amazonaws.com/cdn.growtopiagame.com/website/resources/assets/images/404_bg.png);

                            /* Full height */
                            height: 100%;

                            /* Center and scale the image nicely */
                            background-position: center;
                            background-repeat: no-repeat;
                            background-size: cover;
                            color: #fff;
            }

            .container {
                text-align: center;
                display: table-cell;
                vertical-align: middle;
            }

            .content {
                text-align: center;
                display: inline-block;
            }

            .text {
                font-size: 36px;
                margin-bottom: 40px;
            }
            .title {
                font-size: 275px;
                text-shadow: -8px 8px 0px #006f88;
            }
```

NARASI

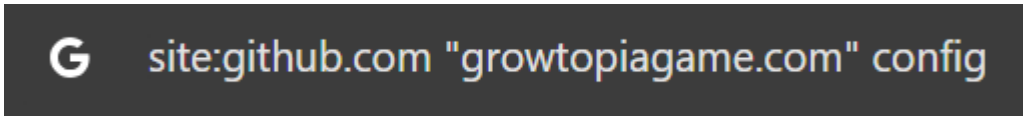
Selanjutnya, dilakukan upaya pencarian file sitemap.xml untuk memetakan struktur konten website. Namun, berdasarkan respons server yang menampilkan kode HTML dengan judul 'Page not found [404]', dapat disimpulkan bahwa situs ini tidak mempublikasikan sitemap di lokasi standar atau memang menyembunyikannya. Hal ini mempersulit pemetaan konten secara otomatis.

c. Analisis HTTP Header (Banner Grabbing)

NARASI

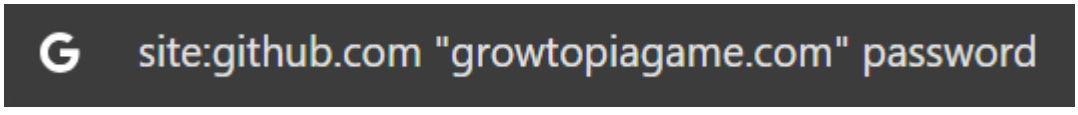
Terakhir, dilakukan analisis HTTP Header menggunakan perintah curl -I. Perintah ini hanya mengambil header respons tanpa mengunduh konten halamannya. Hasil output mengungkapkan bahwa server yang menangani permintaan adalah awselb/2.0, yang mengonfirmasi penggunaan **Amazon Web Services Elastic Load Balancer**. Selain itu, terlihat adanya pengaturan *cookie* AWSALB, yang digunakan untuk menjaga sesi pengguna pada infrastruktur *load balancing* tersebut.

d. Github Dorking



NARASI

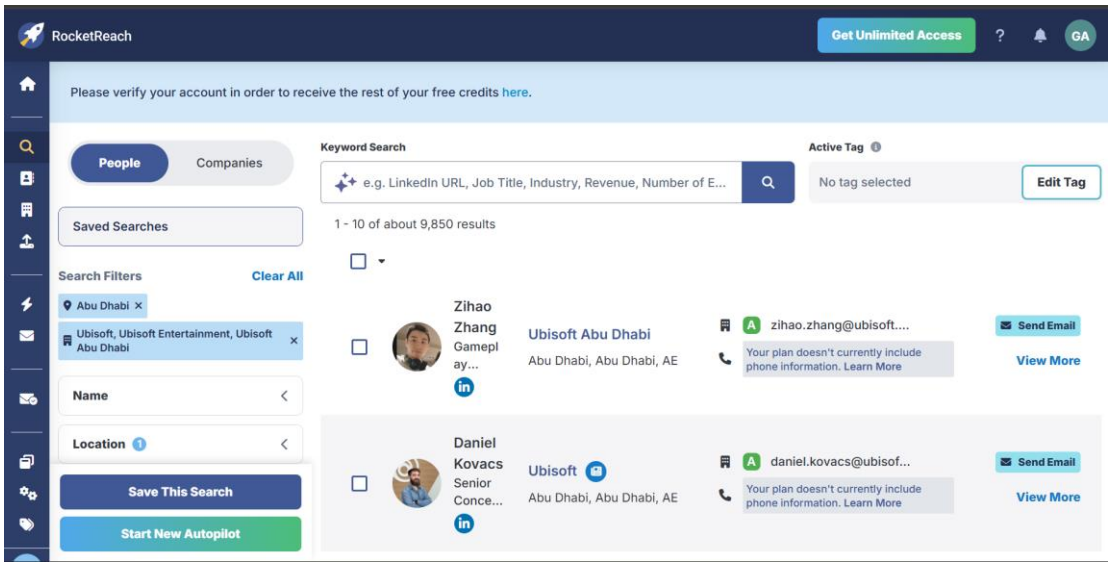
Ditemukan beberapa file konfigurasi di GitHub, namun setelah dianalisis, file tersebut hanyalah konfigurasi untuk bot sisi klien (client-side bots) dan private server, bukan file konfigurasi internal server (server-side config) milik Ubisoft.



NARASI

Pencarian keyword 'password' tidak menemukan kredensial yang bocor. Namun, ditemukan repositori yang memuat source code halaman Phishing (SupportGrowtopia/tapjoysupport) yang menargetkan pemain Growtopia.

9. Identifikasi Karyawan & Kontak



NARASI

Menampilkan nama karyawan yang bekerja pada Ubisoft abu dhabi yang dimana induk dari Perusahaan game growtopia (growtopiagame.com)

Tabel Output Pasif Recon

Informasi yang Ditemukan	**Sumber (Alat/Website)**	**Alasan Relevansi (Penting untuk Serangan)**
Infrastruktur Cloud (AWS Elastic Load Balancer)	Censys & curl -I (Header)	Mengetahui target menggunakan AWS ELB menandakan adanya *firewall* dan fitur *auto-scaling*. Serangan membanjiri trafik (DDoS) ke satu IP akan

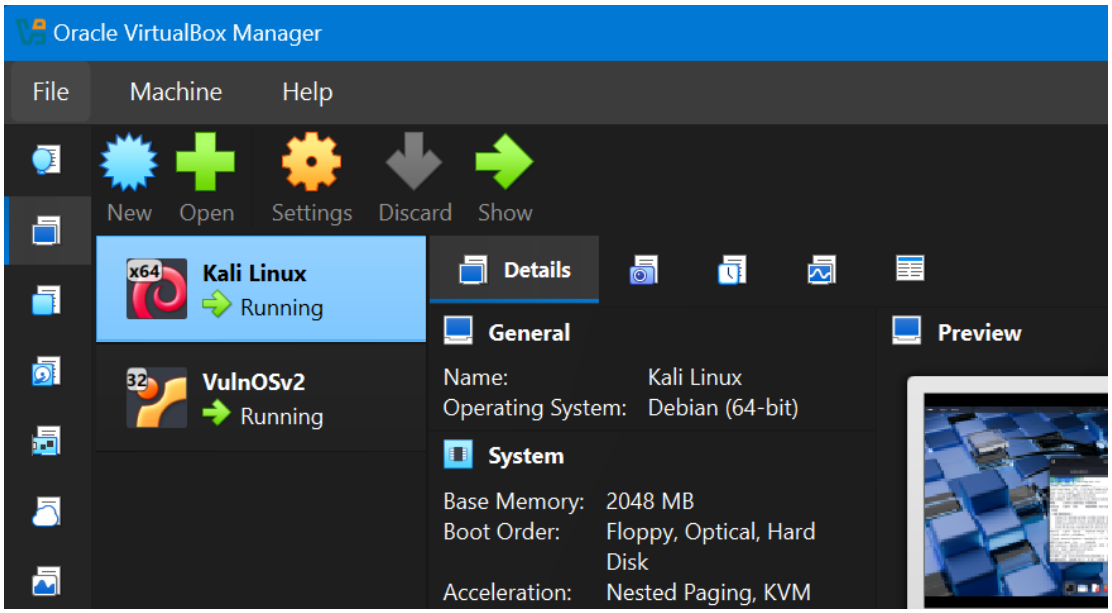
		kurang efektif karena beban dibagi rata.
Lokasi Halaman Admin (/forums/admincp/)	robots.txt	Jalur ini secara eksplisit membuka lokasi pintu masuk administrator forum. Penyerang dapat memfokuskan serangan *Brute Force* atau *Credential Stuffing* langsung ke URL ini.
Subdomain Berisiko (backup., beta., host01.)	Subfinder & Amass	Subdomain seperti 'backup' atau 'beta' sering kali merupakan versi pengembangan yang jarang diperbarui (*unpatched*), sehingga memiliki celah keamanan yang lebih mudah ditembus dibanding domain utama.
Teknologi Forum (vBulletin)	Wappalyzer	Perangkat lunak forum vBulletin memiliki sejarah kerentanan kritis (CVE) yang panjang. Jika versi yang digunakan usang, sistem rentan terhadap serangan *Remote Code Execution* (RCE).

Identitas Personil Kunci (Zihao Zhang, Daniel Kovacs, Reem Fakhouri)	OSINT (LinkedIn/Rocketreach.co)	Informasi nama dan jabatan karyawan teknis sangat krusial untuk menyusun skenario serangan *Social Engineering* atau *Spear Phishing* yang spesifik dan meyakinkan.
Pola Alamat Email (nama.belakang@ubisoft.com)	Analisis Manual / OSINT	Memungkinkan penyerang untuk membuat daftar target email (*email list*) valid guna mengirimkan *malware* atau tautan *phishing* massal ke karyawan internal.
Pemisahan Server Email (IP: 18.206.x.x)	dig MX	Menunjukkan bahwa layanan email ditangani oleh server dengan IP berbeda dari web server. Jika web server sulit ditembus, penyerang bisa mencoba mengeksploitasi server email.
Repositori Phishing (tapjoysupport)	GitHub Search	Meskipun tidak ditemukan kredensial server yang bocor (negatif), ditemukannya *source code* halaman tiruan (*phishing*) di GitHub menandakan adanya kampanye penipuan aktif

		yang menargetkan pengguna Growtopia.

D. Active Recon – Dokumentasi Langkah Per Langkah

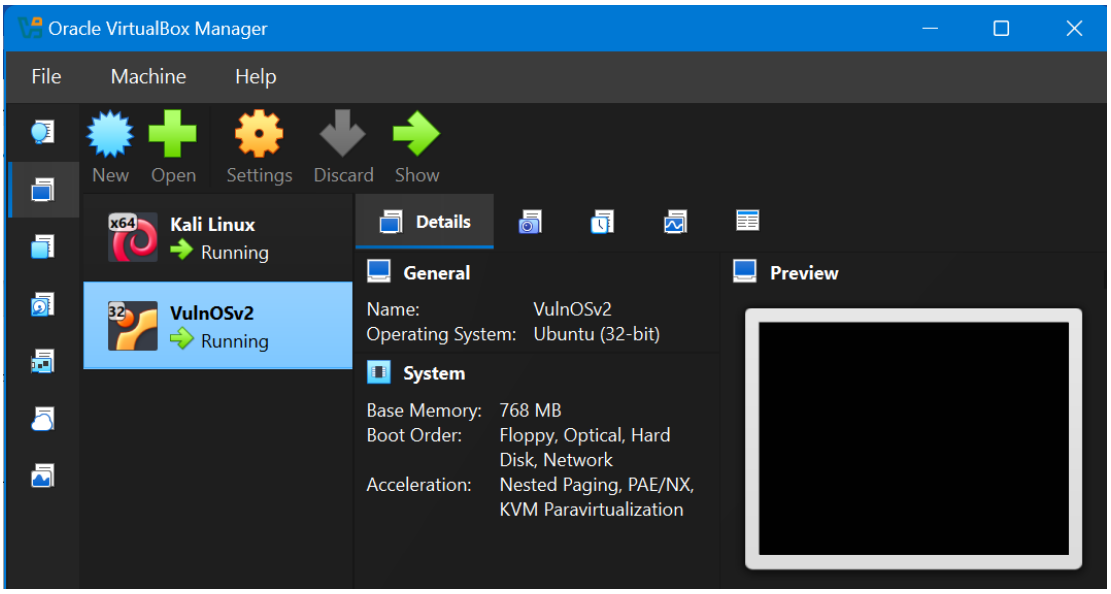
1. Buka Kali Linux



Narasi

Pilih Kali Linux Lali Klik tanda panah

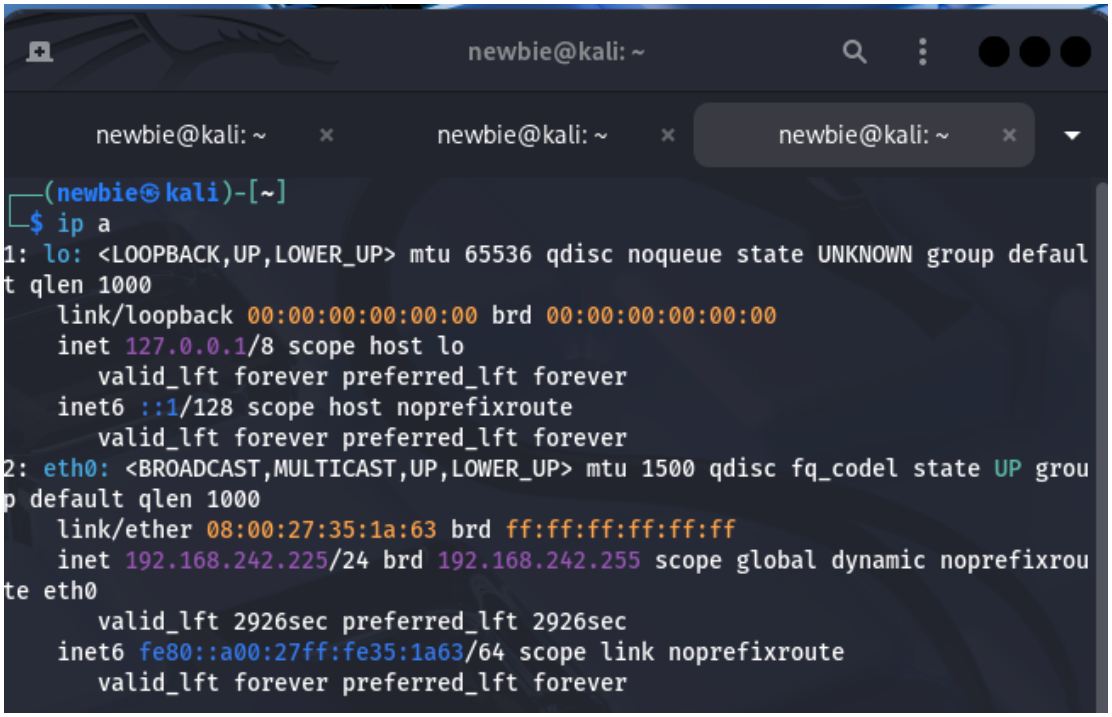
2. **Buka VulnOSv2**



Narasi

pilih Vulnos lalu klik tanda panah

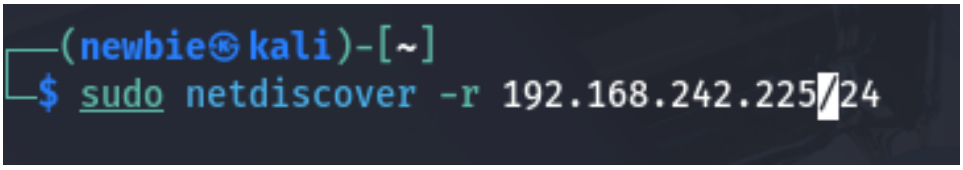
3. **Buka Terminal Kali Linux Untuk Mengetahui ip & subnet**



Narasi

Buka terminal lalu Ketika ip a lalu cari ip kalian sesuai interface masing masing missal saya eth 0 dengan ip 192.168.242.255/24

4. **Jalankan netdiscover untuk memindai seluruh jaringan**



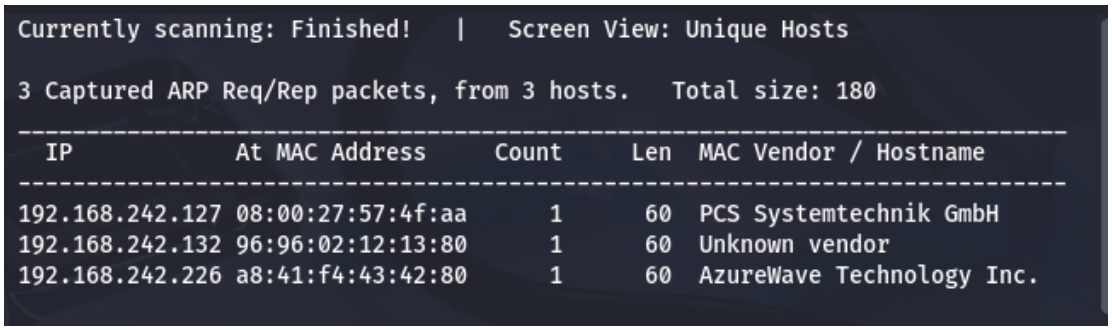
Narasi

Contoh jika IP kamu 192.168.56.10: sudo netdiscover -r 192.168.56.0/24

(sesuaikan dengan ip kalian masing-masing beserta subnet masknya)

Kamu akan melihat daftar IP dan MAC Address. Cari yang Vendor-nya "PCS Systemtechnik" (biasanya VirtualBox) atau "VMware"

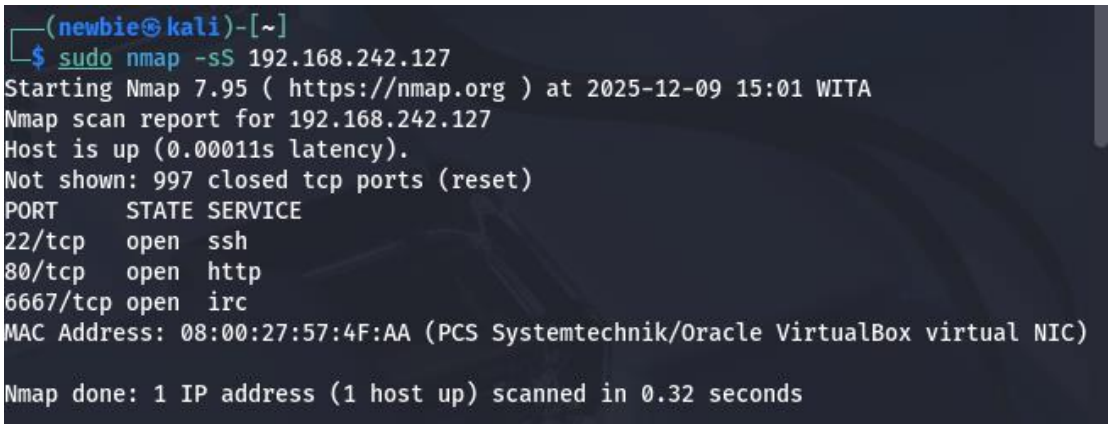
5. **Cari IP Vulons**



NARASI

Cari yang tulisan PCS Systemtechnik GmbH karena itu ip untuk ip vulonosnya,Disini Ip vulnosya 192.168.242.127

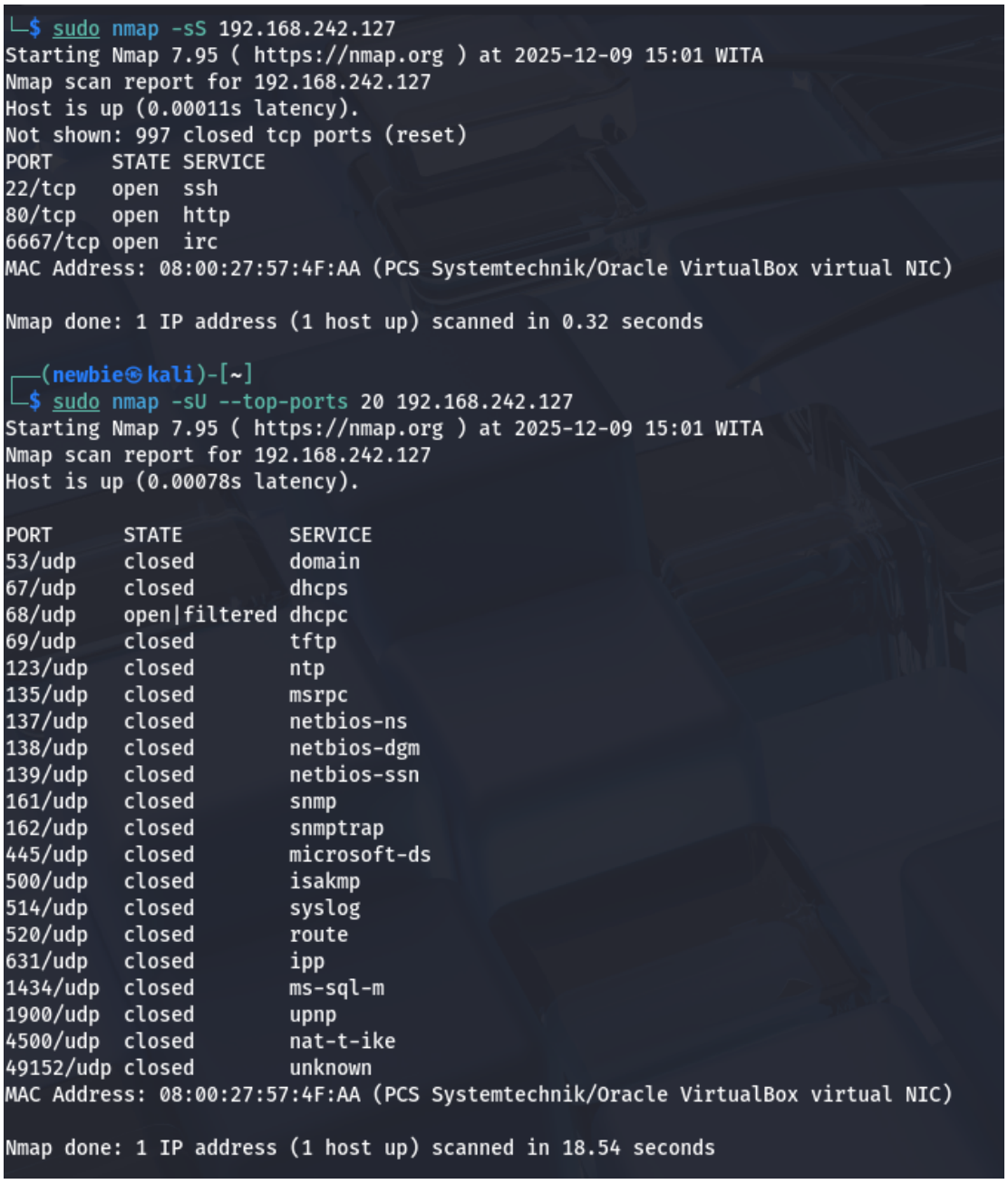
6. **TCP SYN Scan Menggunakan ip vulnos masing masing**



Narasi

Dilakukan pemindaian menggunakan teknik TCP SYN Scan (-sS) yang dikenal sebagai metode *stealthy* karena tidak menyelesaikan proses jabat tangan TCP (*3-way handshake*) secara penuh. Langkah ini bertujuan untuk meminimalkan jejak pada log sistem target. Dari hasil eksekusi perintah tersebut, teridentifikasi tiga port TCP utama yang terbuka, yaitu **Port 22** yang menjalankan layanan SSH untuk akses jarak jauh, **Port 80** yang mengindikasikan keberadaan server web (HTTP), serta **Port 6667** yang menjalankan layanan IRC (*Internet Relay Chat*). Keberadaan layanan IRC ini menjadi temuan menarik karena jarang ditemukan pada konfigurasi server modern dan berpotensi menjadi vektor serangan tambahan.

7. UDP Scan



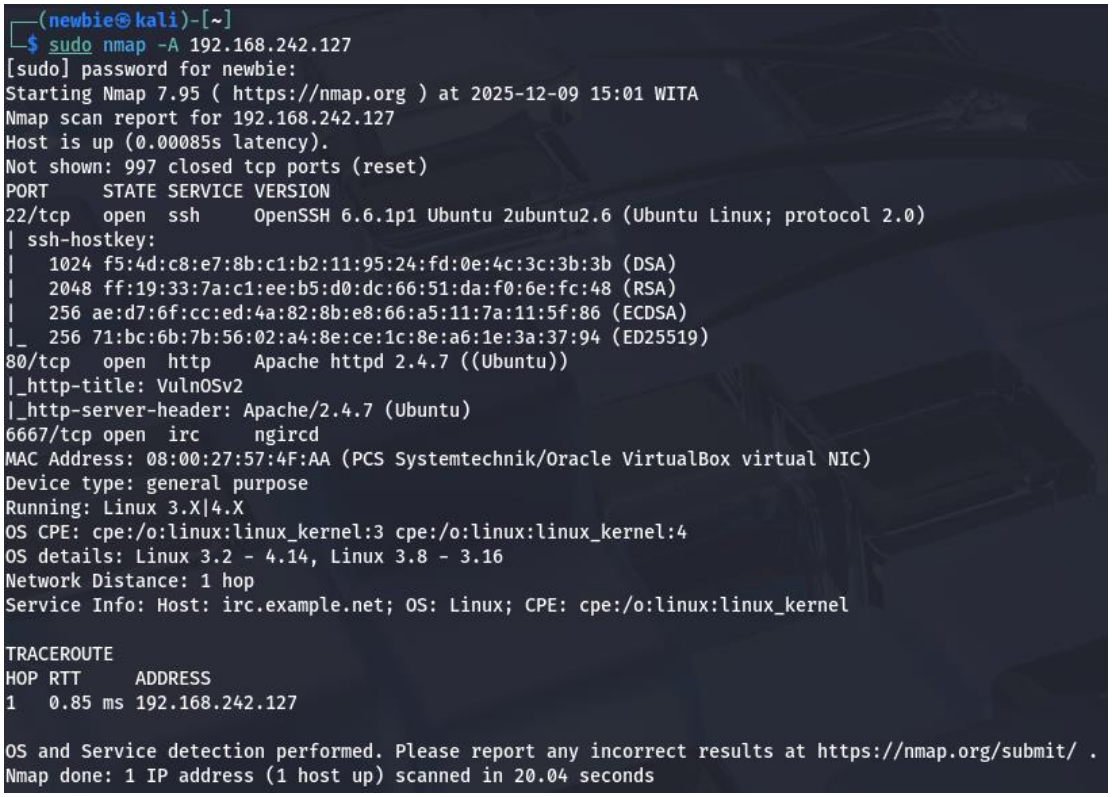
```
└─$ sudo nmap -sS 192.168.242.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 15:01 WITA
Nmap scan report for 192.168.242.127
Host is up (0.00011s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

┌──(newbie㉿kali)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.242.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 15:01 WITA
Nmap scan report for 192.168.242.127
Host is up (0.00078s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
1434/udp  closed        ms-sql-m
1900/udp  closed        upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.54 seconds
```

Narasi

pemindaian diperluas ke protokol UDP menggunakan opsi --top-ports 20 untuk memeriksa 20 port UDP terpopuler. Karena sifat protokol UDP yang *connectionless*, pemindaian jenis ini sering kali tidak mendapatkan respons balik (*ack*), sehingga

status port sering terdeteksi sebagai *open|filtered*. Berdasarkan hasil pemindaian, mayoritas port ditemukan dalam status tertutup (*closed*), kecuali **Port 68** (DHCP Client). Status port ini wajar ditemukan dalam keadaan terbuka karena mesin target dikonfigurasi untuk menerima alamat IP secara otomatis dari jaringan melalui protokol DHCP.

8. **Service Version & OS Detection**



Narasi

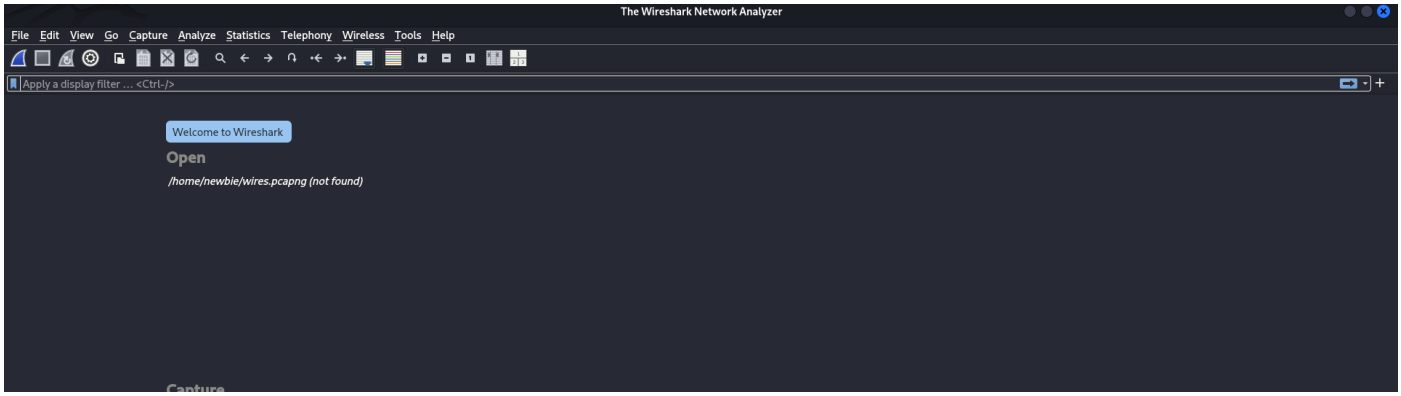
Analisis dilanjutkan ke tahap enumerasi mendalam menggunakan perintah **sudo nmap -A 192.168.242.127**. Perintah ini dipilih karena efisiensinya dalam menggabungkan deteksi versi layanan (*Service Version*) dan identifikasi sistem operasi (*OS Fingerprinting*) dalam satu kali eksekusi, serta menjalankan skrip pemindaian dasar.

Berdasarkan hasil output yang diperoleh, terungkap detail krusial mengenai arsitektur target. Dari sisi layanan, **Port 22** teridentifikasi menjalankan **OpenSSH**

6.6.1p1 (Ubuntu 2ubuntu2.6) dan **Port 80** menjalankan server web **Apache httpd 2.4.7**. Kedua versi perangkat lunak ini tergolong usang (*deprecated*) dan diketahui memiliki berbagai kerentanan publik (CVE). Selain itu, header HTTP pada port 80 secara eksplisit menampilkan judul **"VulnOSv2"**, yang mengonfirmasi identitas target sebagai mesin *vulnerable* VulnOS versi 2.

Secara bersamaan, fitur *OS Fingerprinting* Nmap menganalisis karakteristik paket jaringan dan berhasil mengidentifikasi bahwa target berjalan di atas kernel **Linux (versi 3.2 - 4.14)** pada platform **Ubuntu Linux**. Korelasi antara versi kernel Linux dan paket layanan usang (SSH & Apache) yang ditemukan semakin memperkuat dugaan bahwa sistem operasi yang digunakan adalah varian Ubuntu lawas (kemungkinan besar Ubuntu 14.04 Trusty Tahr), yang menjadi landasan bagi lingkungan lab VulnOS ini.

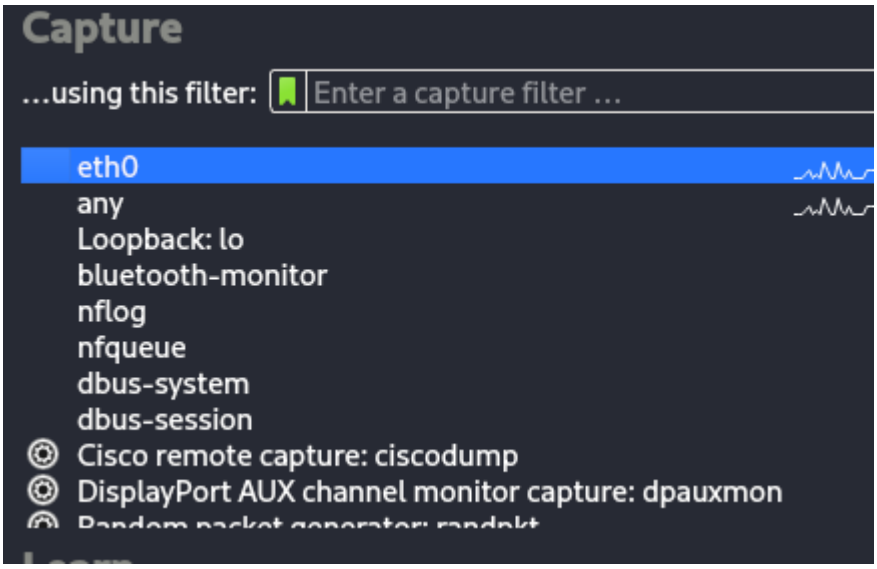
9. **Buka Wireshark**



Narasi

Pilih Icon Gmabar sirip hiu lalu klik 2 kali untuk membuka wireshark

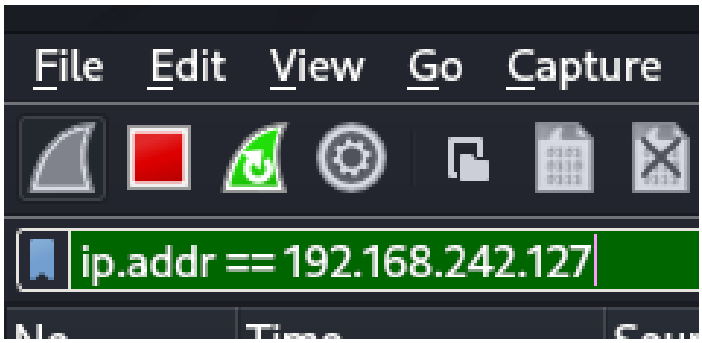
10. Pilih Interface Kalian



Narasi

Disini Interface saya yaitu eth0,lalu klik 2 kali

11. Berikan Filter pada wireshark

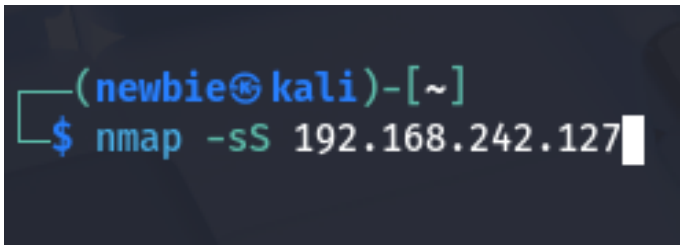


Narasi

Berikan Filter ip.addr == ip vulnos,contoh (ip.addr == 192.168.242.127),lalu enter

Ini digunakan supaya wireshark hanya menampilkan traffic ip kita

12. **Masuk ke terminal dan jalankan nmap sederhana**

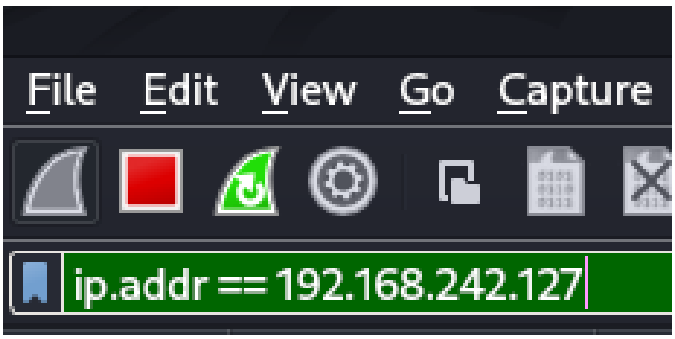



```
(newbie㉿kali)-[~]
$ nmap -sS 192.168.242.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 15:47 WITA
Nmap scan report for 192.168.242.127
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Narasi

Ini untuk wireshark tahu/bisa membaca trafficnya

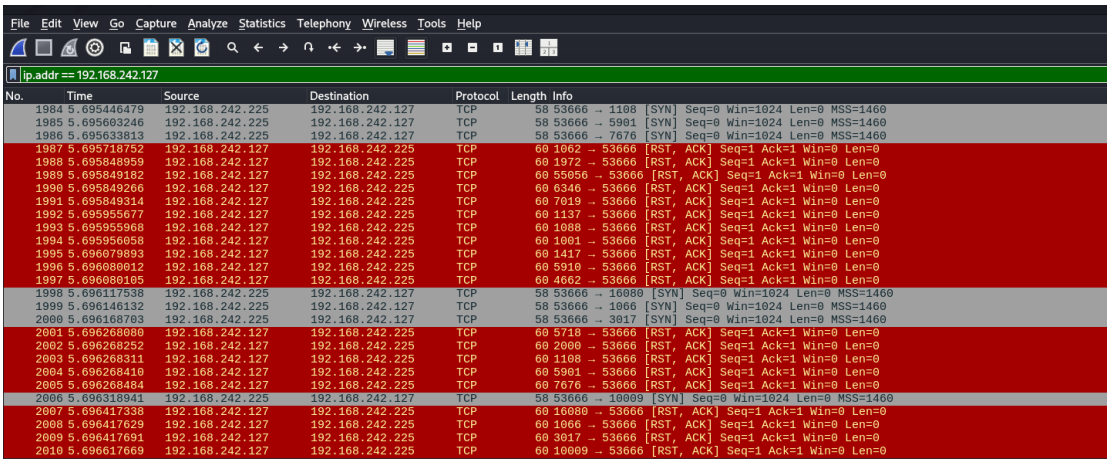
13. **Masuk Kembali ke wireshark dan hentikan capture**



Narasi

Klik to,bol merah kotak untuk menghetikan capture

14. Hasil Traffic



Narasi

Hasil tangkapan layar Wireshark memperlihatkan pola trafik protokol **TCP** yang intensif saat pemindaian Nmap dijalankan. Terlihat jelas paket-paket dengan flag **SYN** dikirimkan oleh penyerang untuk menginisiasi koneksi (*handshake*), yang kemudian direspons oleh target dengan paket **SYN-ACK** (jika port terbuka) atau **RST** (jika port tertutup). Hal ini membuktikan secara visual bagaimana teknik *Active Reconnaissance* bekerja pada level paket jaringan.

E. Kesimpulan Akhir

Berdasarkan serangkaian kegiatan *Reconnaissance* yang telah dilakukan, baik secara pasif terhadap target nyata (growtopiagame.com) maupun secara aktif terhadap target laboratorium (VulnOS), dapat ditarik beberapa kesimpulan penting:

1. **Perbandingan Postur Keamanan**
   a. **Target Pasif (Growtopia/Ubisoft):** Memiliki postur keamanan tingkat *enterprise*. Infrastruktur dilindungi oleh *cloud firewall* AWS dan *Load Balancer*, serta meminimalisir eksposur port. Informasi sensitif dijaga dengan baik (tidak ada kebocoran kredensial di GitHub), namun celah *Information Disclosure* masih ditemukan pada metadata robots.txt dan subdomain lama.

b. **Target Aktif (VulnOS):** Sebagai mesin simulasi, target ini sangat rentan. Ditemukan penggunaan perangkat lunak yang sudah usang (*deprecated*) seperti **OpenSSH 6.6.1** dan **Apache 2.4.7** yang memiliki banyak kerentanan publik (CVE). Selain itu, terbukanya port tidak umum seperti **6667 (IRC)** menandakan potensi *backdoor* atau konfigurasi yang buruk.

2. **Pembelajaran Praktis** Melalui tugas ini, pemahaman mengenai perbedaan metode *Passive* dan *Active* menjadi jelas:
   a. **Passive Recon** sangat berguna untuk memetakan permukaan serangan (*attack surface*) tanpa menyentuh target, sehingga aman dari deteksi IDS/IPS.
   b. **Active Recon** memberikan data teknis yang jauh lebih presisi (versi OS, layanan spesifik), namun menghasilkan jejak lalu lintas jaringan (*noise*) yang mudah dideteksi oleh administrator jaringan, seperti yang terlihat pada analisis trafik Wireshark.

Dokumentasi ini membuktikan bahwa tahap *Reconnaissance* adalah fondasi krusial dalam siklus *Penetration Testing* untuk menentukan vektor serangan yang paling efektif.