

# **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/\\*/](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.
- Mengetahui 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
```

```
(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 <<<
```

```
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

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: 2012-11-06T02:05:43Z
Registrar Registration Expiration 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
Reseller: A
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: UbiSoft Entertainment
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: FR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: b67a2ddbd5e660587e3f8c874ff156da-155864@contact.gandi.net
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
```

## 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 *Registrant Country*nya 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)

```
(newbie㉿kali)-[~]
$ dig growtopiagame.com NS

; <>> DiG 9.20.11-4+b1-Debian <>> growtopiagame.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4333
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
growtopiagame.com.    3467    IN      NS      nic10.ubisoft.com.
growtopiagame.com.    3467    IN      NS      nic8.ubisoft.com.
growtopiagame.com.    3467    IN      NS      nic9.ubisoft.com.
growtopiagame.com.    3467    IN      NS      nic11.ubisoft.com.
growtopiagame.com.    3467    IN      NS      nic12.ubisoft.com.
growtopiagame.com.    3467    IN      NS      nic7.ubisoft.com.

;; Query time: 68 msec
;; SERVER: 192.168.242.132#53(192.168.242.132) (UDP)
;; WHEN: Tue Dec 09 07:41:59 WITA 2025
;; MSG SIZE  rcvd: 171
```

## 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)

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

; <>> DiG 9.20.11-4+b1-Debian <>> growtopiagame.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23303
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
growtopiagame.com.      3443     IN      TXT      "v=spf1 +a +mx +ip4:18.206.25.220 -all"
;; Query time: 52 msec
;; SERVER: 192.168.242.132#53(192.168.242.132) (UDP)
;; WHEN: Tue Dec 09 07:42:23 WITA 2025
;; MSG SIZE  rcvd: 96
```

### 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)

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

[INFO] Loading provider config from /home/newbie/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for growtopiagame.com

projectdiscovery.io

[INFO] Loading provider config from /home/newbie/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for growtopiagame.com
```

```
login.growtopiagame.com
www.growtopiagame.com
mail1.growtopiagame.com
backup.growtopiagame.com
host01.growtopiagame.com
beta.growtopiagame.com
xsolla.growtopiagame.com
static.growtopiagame.com
growtopiagame.com
```

#### 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)

```
(newbie㉿kali)-[~]
└─$ amass enum -passive -d growtopiagame.com
```

```
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

Certificates	<a href="#">Criteria</a>	Type: Identity	Match: ILIKE	Search: 'growtopiagame.com'			
	<a href="#">crt.sh ID</a>	<a href="#">Logged At</a>	<a href="#">Not Before</a>	<a href="#">Not After</a>	<a href="#">Common Name</a>	<a href="#">Matching Identities</a>	<a href="#">Issuer Name</a>
	<a href="#">22778018414</a>	2025-11-28	2025-11-28	2026-02-26	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R12</code>
	<a href="#">22778009763</a>	2025-11-28	2025-11-28	2026-02-26	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R12</code>
	<a href="#">21551771213</a>	2025-10-06	2025-10-06	2026-01-04	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">21522516875</a>	2025-10-06	2025-10-06	2026-01-04	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">21369092298</a>	2025-09-29	2025-09-29	2025-12-28	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">21363075048</a>	2025-09-29	2025-09-29	2025-12-28	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">21206845621</a>	2025-09-22	2025-09-22	2025-12-21	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">21212275815</a>	2025-09-22	2025-09-22	2025-12-21	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R13</code>
	<a href="#">19986518974</a>	2025-07-29	2025-07-29	2025-10-27	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">19986499561</a>	2025-07-29	2025-07-29	2025-10-27	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">19711535039</a>	2025-07-16	2025-07-16	2026-07-16	*.growtopiagame.com	*.growtopiagame.com	<code>C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA OV R36</code>
	<a href="#">19711535334</a>	2025-07-16	2025-07-16	2026-07-16	*.growtopiagame.com	*.growtopiagame.com	<code>C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA OV R36</code>
	<a href="#">19711466132</a>	2025-07-16	2025-07-16	2025-10-14	growtopiagame.com	growtopiagame.com	<code>C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36</code>
	<a href="#">19711465407</a>	2025-07-16	2025-07-16	2025-10-14	growtopiagame.com	growtopiagame.com	<code>C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36</code>
	<a href="#">19287811292</a>	2025-06-27	2025-06-27	2025-09-25	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">19287811285</a>	2025-06-27	2025-06-27	2025-09-25	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">19171755884</a>	2025-06-22	2025-06-22	2025-09-20	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">19171758993</a>	2025-06-22	2025-06-22	2025-09-20	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">18012243012</a>	2025-04-23	2025-04-23	2025-07-22	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">18013215815</a>	2025-04-23	2025-04-23	2025-07-22	xsolla.growtopiagame.com	xsolla.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>
	<a href="#">17578307368</a>	2025-04-02	2025-04-02	2025-07-01	standard-tls- static.cdn.ubi.com	static.growtopiagame.com	<code>C=US, O=Let's Encrypt, CN=R10</code>

## 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)

**Censys**   Register Log In

**Results**

**Host Filters**

Labels:

- 48 remote-access
- 46 file-sharing
- 46 network-administration
- 12 load-balancer
- 1 email
- More

Autonomous System:

- 46 HYONIX Hyonix
- 22 AMAZON-02
- 16 AMAZON-AES
- 2 OVH
- 1 AKAMAI-AS1
- More

Location:

- 68 United States
- 19 Ireland
- 2 Germany
- 1 Indonesia

**Service Filters**

Service Names:

- 230 HTTP
- 46 NETBIOS
- 46 RDP
- 46 SMB
- 44 DCERPC
- More

Ports:

- 85 443
- 65 445

**Hosts**

Results: 90 Time: 0.06s

- 100.25.181.250 (ec2-100-25-181-250.compute-1.amazonaws.com)
  - AMAZON-AES (14618) Virginia, United States
  - load-balancer
  - 80/HTTP
  - 443/HTTP
- 18.206.25.220 (ec2-18-206-25-220.compute-1.amazonaws.com)
  - AMAZON-AES (14618) Virginia, United States
  - email
  - 25/SMTP
  - 587/SMTP
- 98.86.35.186 (ec2-98-86-35-186.compute-1.amazonaws.com)
  - AMAZON-AES (14618) Virginia, United States
  - load-balancer
  - 443/HTTP
- 52.3.20.246
  - AMAZON-AES (14618) Virginia, United States
  - load-balancer
  - 80/HTTP
  - 443/HTTP
- 103.127.133.177 (ip-177-133-127-103.wjv-1.biznetg.io)
  - IDNIC-BIZNETGIO-AS-10 PTT Biznet Gio Nusantara (133800) West Java, Indonesia
  - 80/HTTP
  - 443/HTTP
- 3.222.181.8
  - AMAZON-AES (14618) Virginia, United States
  - load-balancer
  - 80/HTTP
  - 443/HTTP

**100.25.181.250**

As of: Dec 06, 2025 4:11pm UTC | Latent

**Summary** **History** **WHOIS** **Explore** **Raw Data**

**Basic Information**

- Reverse DNS ec2-100-25-181-250.compute-1.amazonaws.com
- Forward DNS growtopiagame.com
- Routing 100.24.0.0/13 via AMAZON-AES US (AS14618)
- Services (2) 80/HTTP, 443/HTTP
- Labels (1) LOAD BALANCER

**HTTP 80/TCP** (LOAD BALANCER)

Software Amazon Elastic Load Balancing 2.0

Details <http://100.25.181.250/>

Status 403 Forbidden

Body Hash sha1:7771ea4e9cdeed92ce2246b5d71bb23ff92b9fbda90

HTML Title 403 Forbidden

Response Body [EXPAND](#)

**HTTP 443/TCP** (LOAD BALANCER)

Software

**Geographic Location**

- City Ashburn
- State Virginia
- Country United States (US)
- Coordinates 39.04372, -77.48749
- Timezone America/New\_York

## 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

The screenshot shows the Wappalyzer interface with the following identified technologies:

- CMS**: WordPress
- Databases**: MySQL
- Message boards**: vBulletin
- Tag managers**: Google Tag Manager
- Analytics**: Google Analytics GA4
- JavaScript libraries**: Masonry, jQuery 2.1.4
- Blogs**: WordPress
- PaaS**: Amazon Web Services
- Security**: HSTS
- Load balancers**: Amazon ALB
- Programming languages**: PHP
- UI frameworks**: Animate.css, Bootstrap 3.3.7
- CDN**: Amazon S3

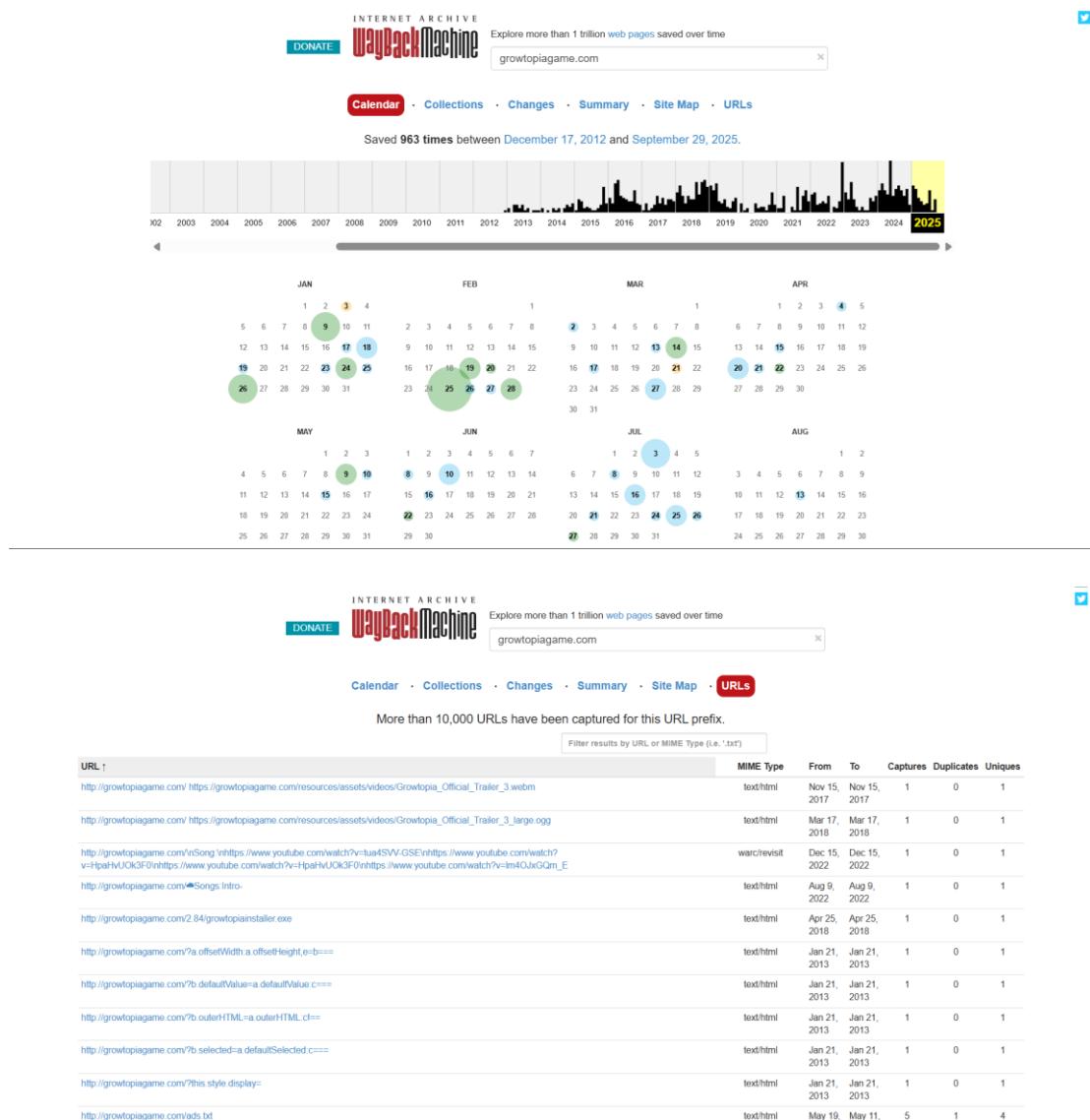
[Something wrong or missing?](#)

## 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 asset (*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 asset-asset 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)

```
(newbie㉿kali)-[~]
└─$ curl -s https://growtopiagame.com/robots.txt

User-agent: Applebot
Disallow: /player/
Disallow: /vanguard/
Disallow: /forums/admincp/
Disallow: /forums/usage/
Disallow: /forums/logs/

User-agent: baiduspider
Disallow: /player/
Disallow: /vanguard/
Disallow: /forums/admincp/
Disallow: /forums/usage/
Disallow: /forums/logs/

User-agent: Bingbot
Disallow: /player/
Disallow: /vanguard/
Disallow: /forums/admincp/
Disallow: /forums/usage/
Disallow: /forums/logs/

User-agent: Discordbot
Disallow: /player/
Disallow: /vanguard/
Disallow: /forums/admincp/
Disallow: /forums/usage/
Disallow: /forums/logs/

User-agent: facebookexternalhit
Disallow: /player/
Disallow: /vanguard/
Disallow: /forums/admincp/
Disallow: /forums/usage/
Disallow: /forums/logs/
```

## 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;
    }
  </style>
</head>
<body>
  <div class="container">
    <div class="content">
      <h1>Page not found [404]</h1>
      <p>The page you were looking for does not exist. Please check the URL or try a different search term.</p>
      <div class="text">It's a trap!</div>
      <div class="title">404</div>
    </div>
  </div>
</body>
</html>
```

## 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)

```
(newbie㉿kali)-[~]
└─$ curl -I https://growtopiagame.com
HTTP/2 502
server: awselb/2.0
date: Mon, 08 Dec 2025 13:44:20 GMT
content-type: text/html
content-length: 122
set-cookie: AWSALB=2KB0MDmqBZmBH2MNKGpC98/LjqybVvX+YgmzBWUN+OJisrNkBgZm4etq0SKrtk26eIy04Ny432kPWiC8HXzZJX+sefzzDMPXlGkQg4YovJXSMABbWJO+TqR0isrL; Expires=Mon, 15 Dec 2025 13:44:20 GMT; Path=/
set-cookie: AWSALBCORS=2KB0MDmqBZmBH2MNKGpC98/LjqybVvX+YgmzBWUN+OJisrNkBgZm4etq0SKrtk26eIy04Ny432kPWiC8HXzZJX+sefzzDMPXlGkQg4YovJXSMABbWJO+TqR0isrL; Expires=Mon, 15 Dec 2025 13:44:20 GMT; Path=/; SameSite=None; Secure
```

### 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

```
G site:github.com "growtopiagame.com" config
```

### 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.

```
G site:github.com "growtopiagame.com" password
```

### 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

The screenshot shows the RocketReach web interface. At the top, there's a message: "Please verify your account in order to receive the rest of your free credits [here](#)". Below this, there are tabs for "People" (selected) and "Companies". A "Keyword Search" bar contains placeholder text "e.g. LinkedIn URL, Job Title, Industry, Revenue, Number of E...". An "Active Tag" section says "No tag selected" with a "Edit Tag" button. On the left, there's a sidebar with various icons and a "Saved Searches" section containing a saved search for "Ubisoft, Ubisoft Entertainment, Ubisoft Abu Dhabi". Below this are "Search Filters" for "Name" and "Location" (set to "Abu Dhabi"). Buttons for "Save This Search" and "Start New Autopilot" are also present. The main results area shows two entries: "Zihao Zhang" (Ubisoft Abu Dhabi) and "Daniel Kovacs" (Ubisoft). Each entry includes a profile picture, name, company, location, email address (with a "Send Email" button), and a note about phone information. There are also "View More" buttons.

### NARASI

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

**Tabel Output Pasif Recon**

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

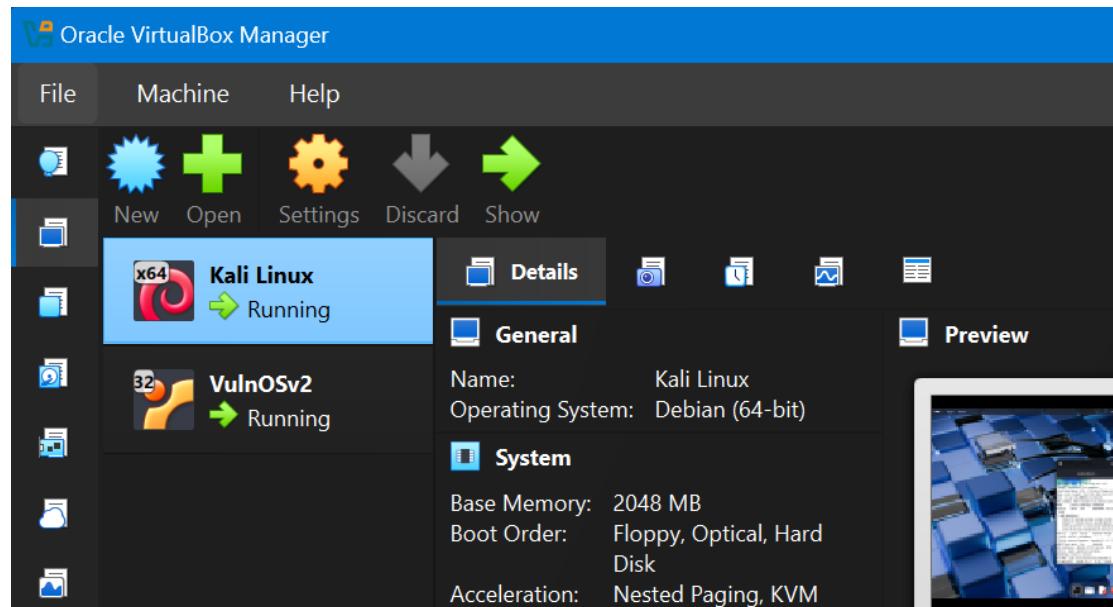
		kurang efektif karena beban dibagi rata.
<b>Lokasi Halaman Admin</b> (/forums/admincp/)	robots.txt	Jalur ini secara eksplisit membuka lokasi pintu masuk administrator forum. Penyerang dapat memfokuskan serangan <i>Brute Force</i> atau <i>Credential Stuffing</i> langsung ke URL ini.
<b>Subdomain Berisiko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

<b>Identitas Personil Kunci</b> (Zihao Zhang, Daniel Kovacs, Reem Fakhouri)	OSINT (LinkedIn/Rocketreach.co)	Informasi nama dan jabatan karyawan teknis sangat krusial untuk menyusun skenario serangan <i>Social Engineering</i> atau <i>Spear Phishing</i> yang spesifik dan meyakinkan.
<b>Pola Alamat Email</b> (nama.belakang@ubisoft.com)	Analisis Manual / OSINT	Memungkinkan penyerang untuk membuat daftar target email ( <i>email list</i> ) valid guna mengirimkan <i>malware</i> atau tautan <i>phishing</i> massal ke karyawan internal.
<b>Pemisahan Server Email</b> (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 mengeksplorasi server email.
<b>Repositori Phishing</b> (tapjoysupport)	GitHub Search	Meskipun tidak ditemukan kredensial server yang bocor (negatif), ditemukannya <i>source code</i> halaman tiruan ( <i>phishing</i> ) di GitHub menandakan adanya kampanye penipuan aktif

yang menargetkan pengguna Growtopia.

## D. Active Recon – Dokumentasi Langkah Per Langkah

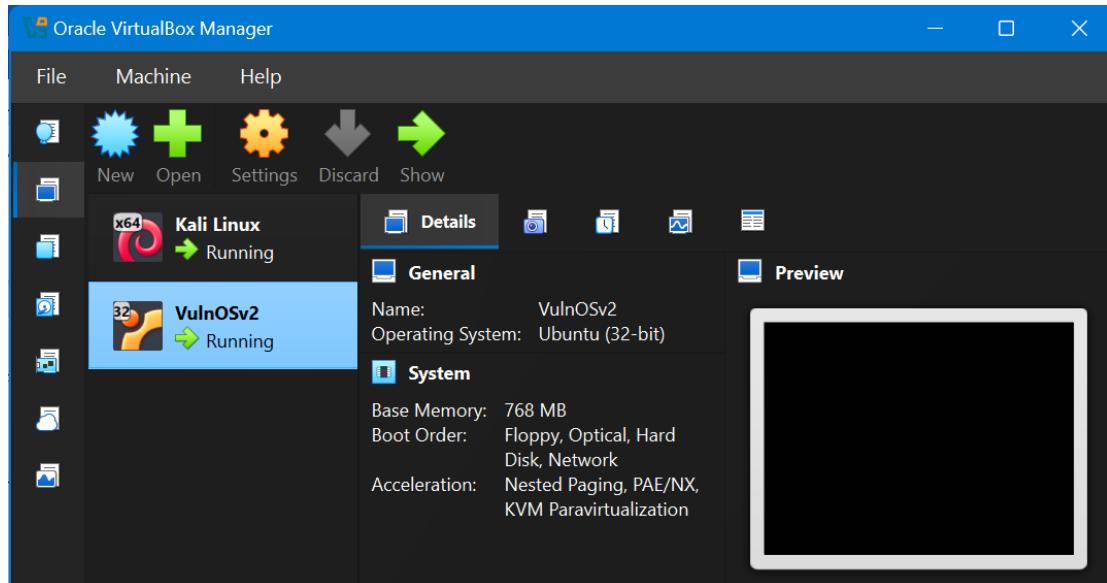
### 1. Buka Kali Linux



#### Narasi

Pilih Kali Linux Lalu Klik tanda panah

## 2. Buka VulnOSv2



### Narasi

pilih Vulnos lalu klik tanda panah

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

A screenshot of a terminal window on Kali Linux. The title bar says 'newbie@kali: ~'. The terminal shows three tabs. The active tab displays the command '\$ ip a' followed by its output. The output shows two interfaces: 'lo' (loopback) and 'eth0' (ethernet). For 'lo', it has an IP of 127.0.0.1/8. For 'eth0', it has an IP of 192.168.242.225/24. Other details like MTU, queueing discipline (qdisc), and link layer information are also provided.

```
(newbie㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:35:1a:63 brd ff:ff:ff:ff:ff:ff
    inet 192.168.242.225/24 brd 192.168.242.255 scope global dynamic noprefixroute
        link-layer brd ff:ff:ff:ff:ff:ff
        valid_lft 2926sec preferred_lft 2926sec
    inet6 fe80::a00:27ff:fe35:1a63/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## 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

```
[newbie@kali:~]
$ sudo netdiscover -r 192.168.242.225/24
```

## 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 Vulns

```
Currently scanning: Finished! | Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

-----

| IP              | At                | MAC Address | Count | Len | MAC Vendor / Hostname     |
|-----------------|-------------------|-------------|-------|-----|---------------------------|
| 192.168.242.127 | 08:00:27:57:4f:aa |             | 1     | 60  | PCS Systemtechnik GmbH    |
| 192.168.242.132 | 96:96:02:12:13:80 |             | 1     | 60  | Unknown vendor            |
| 192.168.242.226 | a8:41:f4:43:42:80 |             | 1     | 60  | AzureWave Technology Inc. |


```

## NARASI

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

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

```
(newbie㉿kali)-[~]
└─$ 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
```

### 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

```
(newbie㉿kali)-[~]
└─$ sudo nmap -A 192.168.242.127
[sudo] password for newbie:
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 (0.00085s latency).

Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 f5:4d:c8:e7:8b:c1:b2:11:95:24:fd:0e:4c:3c:3b:3b (DSA)
|   2048 ff:19:33:7a:c1:ee:b5:d0:dc:66:51:da:f0:6e:fc:48 (RSA)
|   256 ae:d7:6f:cc:ed:4a:82:8b:e8:66:a5:11:7a:11:5f:86 (ECDSA)
|_  256 71:bc:6b:7b:56:02:a4:8e:ce:1c:8e:a6:1e:3a:37:94 (ED25519)

80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: VulnOSv2
|_http-server-header: Apache/2.4.7 (Ubuntu)
6667/tcp  open  irc      ngircd
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.85 ms  192.168.242.127

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.04 seconds
```

### 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.

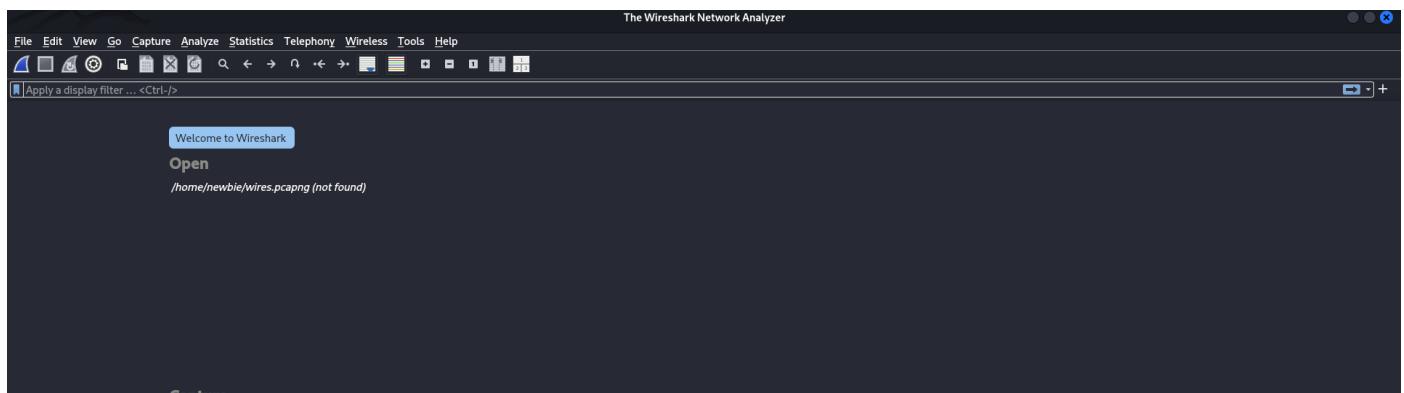
Berdasarkan hasil output yang diperoleh, terungkap detail krusial mengenai arsitektur target. Dari sisi layanan, **Port 22** teridentifikasi menjalankan **OpenSSH**

**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.

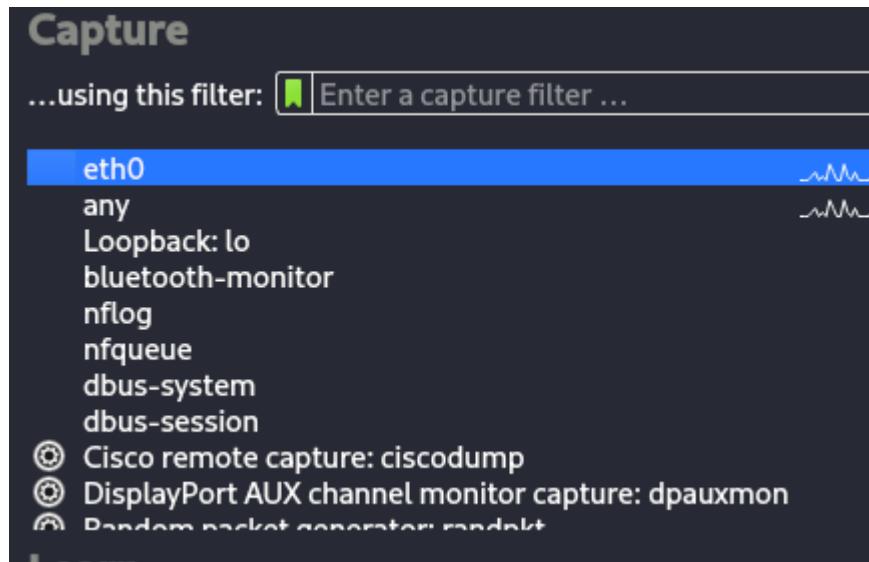
## 9. Buka Wireshark



### Narasi

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

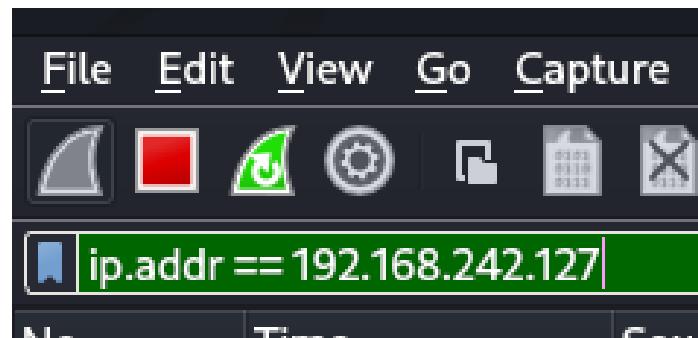
## 10. Pilih Interface Kalian



### 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
```

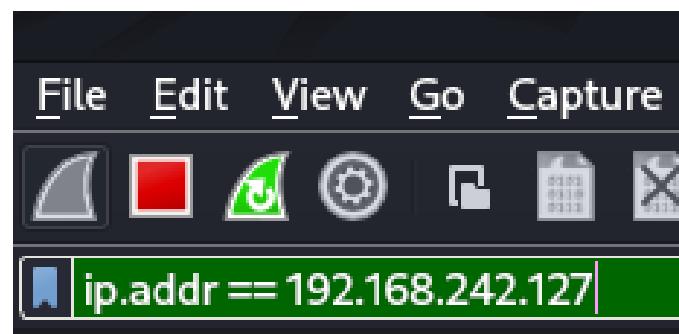
```
(newbie㉿kali)-[~]
$ nmap -sS 192.168.242.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 15:47 WITA
Nmap scan report for 192.168.242.127
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
6667/tcp  open  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 tombol merah kotak untuk menghentikan capture

## 14. Hasil Traffic

No.	Time	Source	Destination	Protocol	Length	Info
1984	5.695446479	192.168.242.225	192.168.242.127	TCP	58	53666 - 1108 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1985	5.695663246	192.168.242.225	192.168.242.127	TCP	58	53666 - 5901 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1986	5.695633813	192.168.242.225	192.168.242.127	TCP	58	53666 - 7676 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1987	5.695718752	192.168.242.127	192.168.242.225	TCP	60	1062 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1988	5.695848959	192.168.242.127	192.168.242.225	TCP	60	1972 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1989	5.695849182	192.168.242.127	192.168.242.225	TCP	60	55956 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1990	5.695849266	192.168.242.127	192.168.242.225	TCP	60	6346 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1991	5.695850214	192.168.242.127	192.168.242.225	TCP	60	7601 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1992	5.695850567	192.168.242.127	192.168.242.225	TCP	60	1047 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1993	5.695955968	192.168.242.127	192.168.242.225	TCP	60	1080 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1994	5.695956058	192.168.242.127	192.168.242.225	TCP	60	1081 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1995	5.696079893	192.168.242.127	192.168.242.225	TCP	60	1417 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1996	5.696088012	192.168.242.127	192.168.242.225	TCP	60	5919 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1997	5.6960880185	192.168.242.127	192.168.242.225	TCP	60	4662 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1998	5.696117538	192.168.242.225	192.168.242.127	TCP	58	53666 - 10880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1999	5.696146132	192.168.242.225	192.168.242.127	TCP	58	53666 - 1066 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2000	5.696168763	192.168.242.225	192.168.242.127	TCP	58	53666 - 3017 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2001	5.696268080	192.168.242.127	192.168.242.225	TCP	60	5718 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2002	5.696268252	192.168.242.127	192.168.242.225	TCP	60	2090 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2003	5.696268311	192.168.242.127	192.168.242.225	TCP	60	1108 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2004	5.696268410	192.168.242.127	192.168.242.225	TCP	60	5991 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2005	5.696268484	192.168.242.127	192.168.242.225	TCP	60	7676 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2006	5.696318943	192.168.242.225	192.168.242.127	TCP	58	53666 - 10809 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2007	5.696417627	192.168.242.225	192.168.242.127	TCP	60	1039 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2008	5.696417629	192.168.242.127	192.168.242.225	TCP	60	1069 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2009	5.696417691	192.168.242.127	192.168.242.225	TCP	60	3017 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2010	5.696617669	192.168.242.127	192.168.242.225	TCP	60	10089 - 53666 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

## 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 direspon 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](http://growtopiagame.com)) maupun secara aktif terhadap target laboratorium (VulnOS), dapat ditarik beberapa kesimpulan penting:

### 1. Perbandingan Postur Keamanan

- 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.