Alejandro García Gutiérrez

Ejercicio 1: Planificación y reconocimiento de una organización

Contenido

[Objetivo del ejercicio 2](#_Toc199060167)

[Diseño y fases del ejercicio: 2](#_Toc199060168)

[Información WHOIS del dominio principal (aubay.com) 3](#_Toc199060169)

[Sistemas autónomos y rangos de red asociados 3](#_Toc199060170)

[Subdominios descubiertos 4](#_Toc199060171)

[Selección y priorización de subdominios relevantes 4](#_Toc199060172)

[Resolución DNS de subdominios seleccionados 5](#_Toc199060173)

[Conclusión 6](#_Toc199060174)

# Objetivo del ejercicio

Identificar activos expuestos públicamente pertenecientes a la empresa Aubay, con especial foco en aquellos que puedan representar un riesgo desde el punto de vista de seguridad. Evaluar su infraestructura externa mediante técnicas de reconocimiento pasivo y validación básica.

## Diseño y fases del ejercicio:

1. **Recolección pasiva** de información mediante WHOIS, BGP y fuentes abiertas.
2. **Enumeración de subdominios** usando wordlists y resolución DNS (MassDNS).
3. **Validación de subdominios activos** mediante resolución A/CNAME (dig, massdns).
4. **Identificación de rangos de red** mediante consulta WHOIS sobre direcciones IP.
5. **Priorización de activos** según su potencial exposición o interés atacante.

# Información WHOIS del dominio principal (aubay.com)

* **Dominio:** aubay.com
* **Registrador:** Gandi SAS
* **ID de IANA del registrador:** 81
* **Fecha de creación:** 24 de marzo de 1998
* **Fecha de expiración:** 23 de marzo de 2033
* **Estado del dominio:**
  + clientTransferProhibited
* **DNSSEC:** No firmado (unsigned)
* **Servidores DNS:**
  + NS-92-A.GANDI.NET
  + NS-113-B.GANDI.NET
  + NS-234-C.GANDI.NET
* **Organización registrante:** Aubay (datos personales redactados)
* **Ubicación registrante:** Île-de-France, Francia
* **Email de contacto ofuscado:** [bcc56e442b4816277eb9a4b95244714b-3455339@contact.gandi.net](mailto:bcc56e442b4816277eb9a4b95244714b-3455339@contact.gandi.net)

# Sistemas autónomos y rangos de red asociados

Para identificar el **Sistema Autónomo (AS o ASN)** asociado a un dominio (o más específicamente a su dirección IP pública), ejecutamos:

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

**Proveedor de IP:** Amazon Data Services France  
**Dirección IP resuelta:** 13.37.165.50  
**Rango IP:** 13.36.0.0 - 13.39.255.255  
**ASN (Sistema Autónomo):** AS16509  
**Titular del ASN:** Amazon.com, Inc.  
**Ubicación geográfica aproximada:** Francia (proveedor: Amazon Data Services France)

**Observaciones:** El dominio aubay.com está alojado en la infraestructura cloud de **Amazon Web Services (AWS)**, dentro del Sistema Autónomo AS16509. Esta IP pertenece a un rango de direcciones gestionado por la filial francesa de Amazon (AMAZON-CDG), lo que sugiere que el servicio está desplegado en una región de AWS ubicada en Europa (probablemente París).

En <https://bgp.he.net/dns/> nos confirma nuestros datos obtenidos:

Texto, Correo electrónico

El contenido generado por IA puede ser incorrecto.

# Subdominios descubiertos

└─$ subfinder -d aubay.com -o aubay\_subs.txt

|  |  |
| --- | --- |
| dark-zeram.aubay.com | gipssi.aubay.com |
| data.aubay.com | webmail.aubay.com |
| kyc34-keren.aubay.com | pops.aubay.com |
| av.aubay.com | mail-keren.aubay.com |
| webconf.aubay.com | sirh.aubay.com |
| ns0.aubay.com | gophish.aubay.com |
| www.sbc-teams.aubay.com | jira.aubay.com |
| img.communication.aubay.com | powerdns.aubay.com |
| planning.aubay.com | mantis.aubay.com |
| sbc-teams.aubay.com | aubay.com |
| att.aubay.com | odyssee.aubay.com |
| ip\_pub\_7.aubay.com | vs.aubay.com |
| ossus.aubay.com | cv.aubay.com |
| financeipc.aubay.com | glpi.aubay.com |
| imaps.aubay.com | blog.aubay.com |
| moncv.aubay.com | proxy-s.aubay.com |
| myaubay.aubay.com | fte-gestion.aubay.com |
| portail.aubay.com | dark-vador.aubay.com |
| ga-gestion.aubay.com | monactivite.aubay.com |
| www.aubay.com | r.communication.aubay.com |
| sip.aubay.com | teamtools.aubay.com |
| e-room.aubay.com | ns1.aubay.com |
| autodiscover.aubay.com | ox.aubay.com |
| record.aubay.com | smtps.aubay.com |
| abcnet.aubay.com |  |

## Selección y priorización de subdominios relevantes

Se han seleccionado cinco subdominios por su potencial relevancia a nivel de seguridad, basándose en su funcionalidad o naturaleza técnica:

1. **gophish.aubay.com**
   * Indica el uso de la herramienta [GoPhish](https://getgophish.com/), usada en campañas de *phishing* de prueba. Puede revelar que hacen simulacros de ingeniería social internamente.
2. **jira.aubay.com**
   * Podría contener información sobre proyectos internos, incidencias, desarrollo o gestión. Muchas veces tiene credenciales débiles o acceso público por error.
3. **glpi.aubay.com**
   * GLPI es una herramienta ITSM (gestión de incidencias, inventario, activos, etc.). Puede contener información de infraestructura, usuarios o tickets técnicos.
4. **webmail.aubay.com**
   * Punto de entrada a la mensajería corporativa. De interés para el vector inicial en simulaciones de ataque (password spraying, phishing, etc.).
5. **myaubay.aubay.com**
   * Parece un portal personalizado, posiblemente para empleados o clientes. Suele tener inicio de sesión y podría dar pistas de arquitectura interna.

## Resolución DNS de subdominios seleccionados

Hemos escogido los 5 subdominios más interesantes y les vamos sacar sus IPs publicas  


Texto

El contenido generado por IA puede ser incorrecto.

El resultado confirma que **Aubay tiene al menos un rango de IPs asignado directamente** (aunque es pequeño). Este bloque está **asignado por COLT**, que es el proveedor de conectividad, pero administrado y utilizado por Aubay.

**Información clave que has obtenido:**

* **Subdominio funcional:** glpi.aubay.com
* **Alias CNAME:** ip\_pub\_7.aubay.com
* **IP final:** 213.41.101.7
* **Rango asignado a Aubay:** 213.41.101.0/28 (16 IPs posibles)
* **Proveedor:** COLT
* **ASN asociado al bloque grande:** AS8220 (COLT France)

## Conclusión

En este ejercicio se realizó una breve investigación sobre la empresa Aubay, identificando sus activos digitales clave como sistemas autónomos, rangos de red, dominios y subdominios relevantes. Se priorizaron y analizaron los subdominios más significativos para la enumeración pasiva y activa, obteniendo información valiosa sobre servicios expuestos y posibles vectores de acceso. Sin realizar pruebas agresivas, se identificaron riesgos potenciales relacionados con la exposición de plataformas internas y servicios críticos, lo que subraya la importancia de aplicar medidas de seguridad adecuadas para mitigar posibles ataques.