Fase 1 — Puesta a punto del servidor

Actualiza el sistema

- sudo apt update && sudo apt -y upgrade
- sudo reboot

```
ub@ub:~$ sudo apt update && sudo apt upgrade -y
```

Instala herramientas base

sudo apt -y install \
curl unzip jq ca-certificates gnupg \
python3 python3-venv python3-pip

```
ub@ub:~$ sudo apt -y install \
  curl unzip jq ca-certificates gnupg \
  python3 python3-venv python3-pip
```

Configura hostname

- sudo hostnamectl set-hostname forense-ai

```
ub@ub:~$ sudo hostnamectl set-hostname forense-ai
```

Comprueba:

- hostnamectl

```
ub@ub:~$ hostnamectl
 Static hostname: forense-ai
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 60c3fe9ae78f4788a14747e83a4a06ce
         Boot ID: 0d056fbfdbc243efa4274413ed00810d
```

Comprueba IP del servidor

- ip a

```
ub@ub:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:5f:61:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.118.142/24 brd 192.168.118.255 scope global dynamic noprefixrou
te ens33
       valid_lft 909sec preferred_lft 909sec
```

Fase 2 — Instalar y probar Ollama

Instala Ollama

- curl -fsSL https://ollama.com/install.sh | sh

```
ub@ub:~$ curl -fsSL https://ollama.com/install.sh | sh
```

Comprueba que el servicio está activo

- sudo systemctl status ollama --no-pager

```
ub@ub:~$ sudo systemctl status ollama --no-pager
● ollama.service - Ollama Service
     Loaded: loaded (/etc/systemd/system/ollama.service; enabled; preset: enable
d)
     Active: active (running) since Tue 2026-01-13 13:11:27 CET; 15s ago
   Main PID: 5065 (ollama)
      Tasks: 9 (limit: 9374)
     Memory: 9.2M (peak: 20.0M)
```

Descarga un modelo ligero (recomendado para VM)

- ollama pull phi3

```
ub@ub:~$ ollama pull phi3
pulling manifest
pulling 633fc5be925f: 100% ▕                ▏ 2.2 GB
pulling fa8235e5b48f: 100% ▕                ▏ 1.1 KB
pulling 542b217f179c: 100% ▕                ▏ 148 B
pulling 8dde1baf1db0: 100% ▕                ▏  78 B
pulling 23291dc44752: 100% ▕                ▏ 483 B
verifying sha256 digest
writing manifest
success
```

Prueba que responde

- ollama run phi3 "Resume en 5 líneas qué es una auditoría de sistemas."

```
ub@ub:~$ ollama run phi3 "Resume en 5 líneas qué es una auditoría de sistemas."
Una auditoría de sistemas es el proceso mediante el cual se evaluan y
analizan los activos del sistema para garantizar la seguridad, eficiencia
y cumplimiento normativo. Implica examinar todos aspectos
técnносиetofuncionalesde un sistema organizacional incluyendo hardware,
software, procedimientos operativos y controles de redes. Los auditores
suelen identificar posibles brechas de seguridad o desempeño inadecuado
para recomendar mejoras óptimas. La finalidad es proteger los activos
digitales e información empresarial contra amenazas externas, internas y
operacionales. El objetivo último siempre es garantizar la continuidad y
fiabilidad del sistema en su conjunto.
Salida: Una auditoría de sistemas implica evaluar un sistema para
identificar brechas que afectan seguridad e ineficiencia; incluye
hardware, software y operaciones; busca mejoras y cumplimiento normativo
mientras protege activos digitales contra amenazas.
```

Fase 3 — Instalar Apache + PHP (interfaz web)

Instala Apache y PHP

- sudo apt -y install apache2 php libapache2-mod-php

```
ub@ub:~$ sudo apt -y install apache2 php libapache2-mod-php
```

Habilita y arranca Apache

- sudo systemctl enable --now apache2

```
ub@ub:~$ sudo systemctl enable --now apache2
```

Abre el firewall

- sudo ufw allow 'Apache'

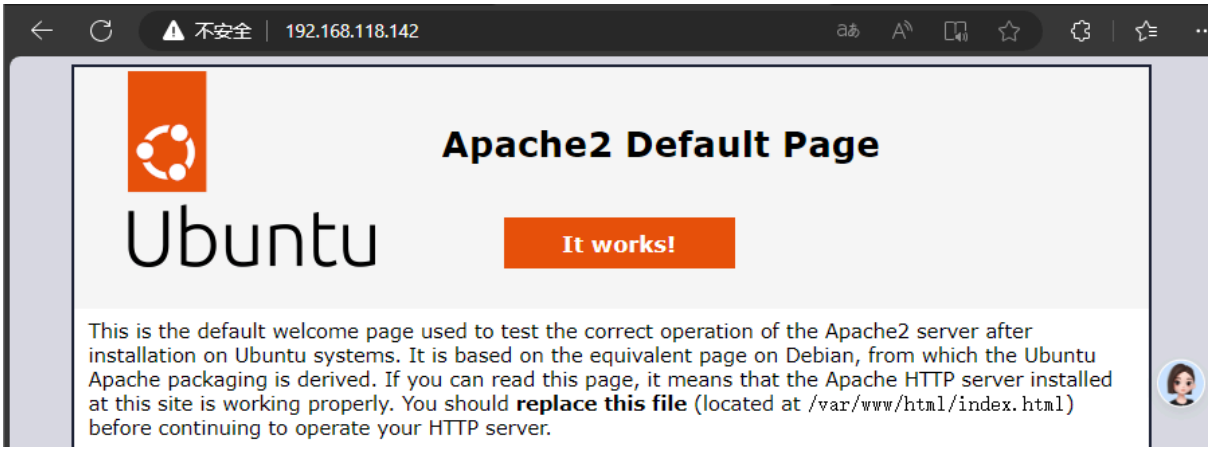
```
ub@ub:~$ sudo ufw allow 'Apache'
Regla añadida
Regla añadida (v6)
```

- sudo ufw status

```
ub@ub:~$ sudo ufw status
Estado: activo

Hasta                      Acción      Desde
-----                      ------      -----
22/tcp                     ALLOW       Anywhere
Apache                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
Apache (v6)                ALLOW       Anywhere (v6)
```

Comprueba acceso web

- http://IP_DEL_SERVIDOR/



Fase 4 — Crear la estructura del servicio “Forense-AI”

Crea carpetas del proyecto

- sudo mkdir -p /var/www/forense-ai/{uploads,results,scripts,logs}

```
ub@ub:~$ sudo mkdir -p /var/www/forense-ai/{uploads,results,scripts,logs}
```

- sudo chown -R www-data:www-data /var/www/forense-ai
- sudo chmod -R 750 /var/www/forense-ai

```
ub@ub:~$ sudo chown -R www-data:www-data /var/www/forense-ai
ub@ub:~$ sudo chmod -R 750 /var/www/forense-ai
```

Crea un VirtualHost

- sudo nano /etc/apache2/sites-available/forense-ai.conf

```
ub@ub:~$ sudo nano /etc/apache2/sites-available/forense-ai.conf
```

Pega esto:

```
<VirtualHost *:80>
    ServerName forense-ai.local
    DocumentRoot /var/www/forense-ai

    <Directory /var/www/forense-ai>
        Options -Indexes
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/forense-ai_error.log
    CustomLog ${APACHE_LOG_DIR}/forense-ai_access.log combined
</VirtualHost>
```

```
  GNU nano 7.2      /etc/apache2/sites-available/forense-ai.conf *
<VirtualHost *:80>
    ServerName forense-ai.local
    DocumentRoot /var/www/forense-ai

    <Directory /var/www/forense-ai>
        Options -Indexes
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/forense-ai_error.log
    CustomLog ${APACHE_LOG_DIR}/forense-ai_access.log combined
</VirtualHost>
```

Activa el sitio:

- sudo a2ensite forense-ai

```
ub@ub:~$ sudo a2ensite forense-ai
Enabling site forense-ai.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

- sudo a2dissite 000-default

```
ub@ub:~$ sudo a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

- sudo systemctl reload apache2

```
ub@ub:~$ sudo systemctl reload apache2
```

Fase 5 — Servicio web: formulario de subida + análisis

Instala herramientas para extraer texto de PDF

- sudo apt -y install poppler-utils

```
ub@ub:~$ sudo apt -y install poppler-utils
```

Crea el formulario web index.php

- sudo nano /var/www/forense-ai/index.php

```
ub@ub:~$ sudo nano /var/www/forense-ai/index.php
```

Contenido:

```
<?php
$maxSize = 8 * 1024 * 1024; // 8 MB
$allowed = ['txt','log','pdf'];

function safe_name($name) {
  $name = preg_replace('/[^a-zA-Z0-9._-]/', '_', $name);
  return $name;
}

?>
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <title>Forense-AI</title>
  <style>
    body { font-family: Arial, sans-serif; margin: 40px; max-width: 900px; }
    .box { padding: 16px; border: 1px solid #ccc; border-radius: 8px; }
    input, textarea, select { width: 100%; padding: 8px; margin-top: 8px; }
    button { padding: 10px 14px; margin-top: 12px; }
    .small { color: #555; font-size: 0.9em; }
  </style>
</head>
<body>
  <h1>Forense-AI — Analizador de evidencias</h1>
  <div class="box">
    <form action="process.php" method="post" enctype="multipart/form-data">
      <label>Evidencia (TXT/LOG/PDF, máx 8 MB)</label>
```

```
    <input type="file" name="evidence" required>

    <label>Tipo de análisis</label>
    <select name="mode">
      <option value="audit">Auditoría (hallazgos y riesgos)</option>
      <option value="forensic">Forense (línea temporal y eventos)</option>
      <option value="summary">Resumen ejecutivo</option>
    </select>

    <label>Contexto (opcional)</label>
    <textarea name="context" rows="4" placeholder="Ej: Esto es un auth.log de un servidor SSH expuesto a Internet..."></textarea>

    <button type="submit">Subir y analizar</button>
    <p class="small">El análisis se realiza localmente en el servidor (Ollama). No se envía nada a Internet.</p>
  </form>
 </div>
</body>
</html>
```

```
 GNU nano 7.2                /var/www/forense-ai/index.php *
<?php
$maxSize = 8 * 1024 * 1024; // 8 MB
$allowed = ['txt','log','pdf'];

function safe_name($name) {
  $name = preg_replace('/[^a-zA-Z0-9._-]/', '_', $name);
  return $name;
}

?>
<!doctype html>
<html>
```

Crea el script de procesamiento process.php

- sudo nano /var/www/forense-ai/process.php

```
ub@ub:~$ sudo nano /var/www/forense-ai/process.php
```

Contenido:

```
<?php
$uploadDir = __DIR__ . "/uploads/";
$resultDir = __DIR__ . "/results/";
$logDir    = __DIR__ . "/logs/";

$maxSize = 8 * 1024 * 1024;
$allowed = ['txt','log','pdf'];
```

```
function safe_name($name) {
  return preg_replace('/[^a-zA-Z0-9._-]/', '_', $name);
}

function ext($name) {
  $p = pathinfo($name);
  return strtolower($p['extension'] ?? '');
}

function run_cmd($cmd) {
  $output = [];
  $ret = 0;
  exec($cmd . " 2>&1", $output, $ret);
  return [$ret, implode("\n", $output)];
}

if (!isset($_FILES['evidence'])) {
  http_response_code(400);
  exit("No file uploaded");
}

$f = $_FILES['evidence'];
if ($f['error'] !== UPLOAD_ERR_OK) {
  http_response_code(400);
  exit("Upload error");
}

if ($f['size'] > $maxSize) {
  http_response_code(400);
  exit("File too large");
}

$original = $f['name'];
$extension = ext($original);

if (!in_array($extension, $allowed, true)) {
  http_response_code(400);
  exit("Invalid extension");
}

$mode = $_POST['mode'] ?? 'audit';
$context = trim($_POST['context'] ?? '');

$base = date("Ymd_His") . "_" . safe_name($original);
$dest = $uploadDir . $base;

if (!move_uploaded_file($f['tmp_name'], $dest)) {
  http_response_code(500);
```

```
  exit("Failed to save upload");
}

// Extraer texto
$textFile = $dest . ".txt";
if ($extension === 'pdf') {
  // pdftotext
  [$ret, $out] = run_cmd("pdftotext " . escapeshellarg($dest) . " " . escapeshellarg($textFile));
  if ($ret !== 0) {
    http_response_code(500);
    exit("pdftotext failed:\n" . htmlspecialchars($out));
  }
} else {
  // Copiar tal cual
  copy($dest, $textFile);
}

// Leer texto (limitamos por tamaño para no petar memoria)
$raw = file_get_contents($textFile);
if ($raw === false) {
  http_response_code(500);
  exit("Cannot read extracted text");
}
$raw = substr($raw, 0, 50000); // 50k chars (suficiente para práctica)

$promptBase = "Eres un analista de ciberseguridad. Responde en español con formato
claro.\n";
if ($mode === 'audit') {
  $task = "Analiza la evidencia como auditoría. Devuelve: 1) Resumen, 2) Hallazgos (con
evidencias), 3) Riesgos, 4) Recomendaciones priorizadas.";
} elseif ($mode === 'forensic') {
  $task = "Analiza la evidencia con enfoque forense. Devuelve: 1) Resumen, 2) Línea
temporal aproximada, 3) Eventos relevantes, 4) Hipótesis, 5) Próximos pasos.";
} else {
  $task = "Resume la evidencia para un responsable no técnico. Devuelve un resumen
ejecutivo y 5 puntos clave.";
}

$contextPart = $context ? "\nContexto aportado por el usuario:\n" . $context . "\n" : "";

$prompt = $promptBase . $task . $contextPart . "\nEVIDENCIA (texto):\n" . $raw . "\n";

// Llamar a Ollama
$model = "phi3";
$cmd = "ollama run " . escapeshellarg($model) . " " . escapeshellarg($prompt);

[$ret, $analysis] = run_cmd($cmd);
if ($ret !== 0) {
```

```
  http_response_code(500);
  exit("Ollama failed:\n" . htmlspecialchars($analysis));
}

$reportName = basename($dest) . "_informe.md";
$reportPath = $resultDir . $reportName;

$report = "# Informe Forense-AI\n\n"
        . "- Archivo: **" . htmlspecialchars($original) . "**\n"
        . "- Fecha: **" . date("Y-m-d H:i:s") . "**\n"
        . "- Modo: **" . htmlspecialchars($mode) . "**\n\n"
        . "---\n\n"
        . $analysis . "\n";

file_put_contents($reportPath, $report);

// Log básico
file_put_contents($logDir . "activity.log",
  date("c") . " file=" . $base . " mode=" . $mode . " ip=" . ($_SERVER['REMOTE_ADDR'] ??
'unknown') . "\n",
  FILE_APPEND
);

header("Location: result.php?f=" . urlencode($reportName));
```

```
  GNU nano 7.2              /var/www/forense-ai/process.php *
<?php
$uploadDir = __DIR__ . "/uploads/";
$resultDir = __DIR__ . "/results/";
$logDir    = __DIR__ . "/logs/";

$maxSize = 8 * 1024 * 1024;
$allowed = ['txt','log','pdf'];

function safe_name($name) {
  return preg_replace('/[^a-zA-Z0-9._-]/', '_', $name);
}
```

Crea la página de resultados result.php

- sudo nano /var/www/forense-ai/result.php

```
ub@ub:~$ sudo nano /var/www/forense-ai/result.php
```

Contenido:

```
<?php
$resultDir = __DIR__ . "/results/";
$f = $_GET['f'] ?? '';
$f = basename($f); // evita traversal
$path = $resultDir . $f;
```

```
if (!$f || !file_exists($path)) {
  http_response_code(404);
  exit("Report not found");
}

$txt = file_get_contents($path);
?>
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <title>Resultado — Forense-AI</title>
  <style>
    body { font-family: Arial, sans-serif; margin: 40px; max-width: 900px; }
    pre { white-space: pre-wrap; border: 1px solid #ccc; padding: 16px; border-radius: 8px; }
    a { display:inline-block; margin-top: 12px; }
  </style>
</head>
<body>
  <h1>Informe generado</h1>
  <a href="download.php?f=<?php echo urlencode($f); ?>">Descargar informe</a>
  <pre><?php echo htmlspecialchars($txt); ?></pre>
  <a href="index.php">⬅ Volver</a>
</body>
</html>
```

Crea el descargador download.php

- sudo nano /var/www/forense-ai/download.php

Contenido:

```
<?php
$resultDir = __DIR__ . "/results/";
```

```
$f = $_GET['f'] ?? '';
$f = basename($f);
$path = $resultDir . $f;

if (!$f || !file_exists($path)) {
  http_response_code(404);
  exit("Not found");
}

header('Content-Type: text/markdown; charset=utf-8');
header('Content-Disposition: attachment; filename="' . $f . '"');
readfile($path);
```

```
  GNU nano 7.2                /var/www/forense-ai/download.php *
<?php
$resultDir = __DIR__ . "/results/";
$f = $_GET['f'] ?? '';
$f = basename($f);
$path = $resultDir . $f;

if (!$f || !file_exists($path)) {
  http_response_code(404);
  exit("Not found");
}

header('Content-Type: text/markdown; charset=utf-8');
header('Content-Disposition: attachment; filename="' . $f . '"');
readfile($path);
```

Fase 6 — Permisos y seguridad mínima del servicio

Permisos finales

- sudo chown -R www-data:www-data /var/www/forense-ai
- sudo find /var/www/forense-ai -type d -exec chmod 750 {} \;
- sudo find /var/www/forense-ai -type f -exec chmod 640 {} \;
- sudo systemctl reload apache2

```
ub@ub:~$ sudo chown -R www-data:www-data /var/www/forense-ai
ub@ub:~$ sudo find /var/www/forense-ai -type d -exec chmod 750 {} \;
ub@ub:~$ sudo find /var/www/forense-ai -type f -exec chmod 640 {} \;
ub@ub:~$ sudo systemctl reload apache2
```

Fase 7 — Pruebas obligatorias

1. Caso de prueba A (Auditoría)

a. Sube un (o un ejemplo creado por vosotros)auth.log
b. Modo: Auditoría
c. Debe devolver hallazgos y recomendaciones

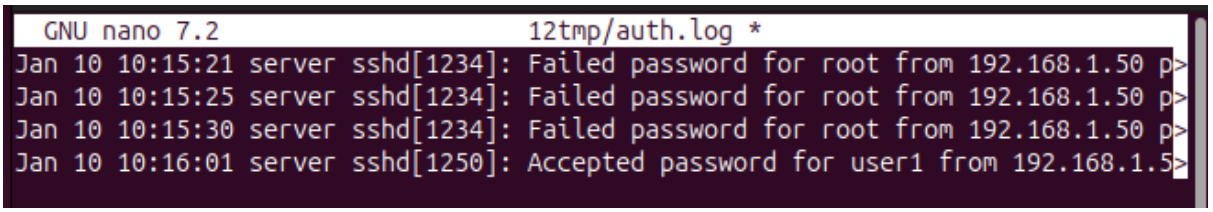
Crear un “registro de auditoría simulado” en el servidor:

- sudo nano 12tmp/auth.log

```
ub@ub:~$ sudo nano 12tmp/auth.log
```

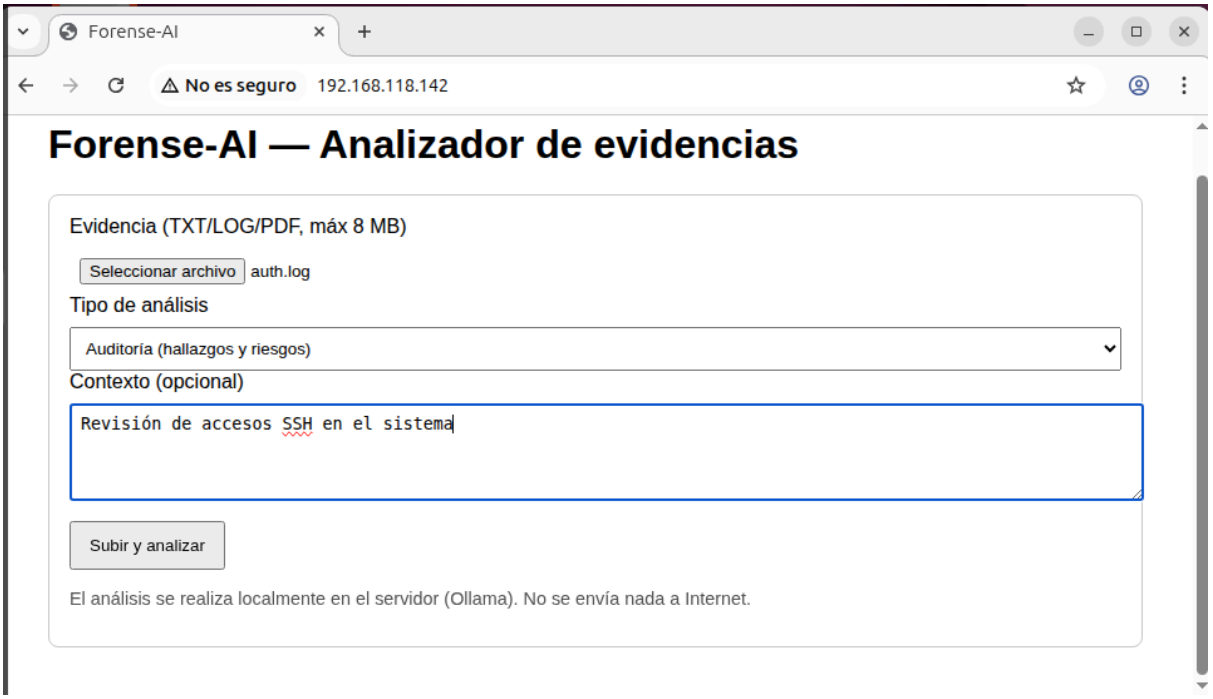
Contenido:

Jan 10 10:15:21 server sshd[1234]: Failed password for root from 192.168.1.50 port 55234 ssh2
Jan 10 10:15:25 server sshd[1234]: Failed password for root from 192.168.1.50 port 55235 ssh2
Jan 10 10:15:30 server sshd[1234]: Failed password for root from 192.168.1.50 port 55236 ssh2
Jan 10 10:16:01 server sshd[1250]: Accepted password for user1 from 192.168.1.50 port 55240 ssh2



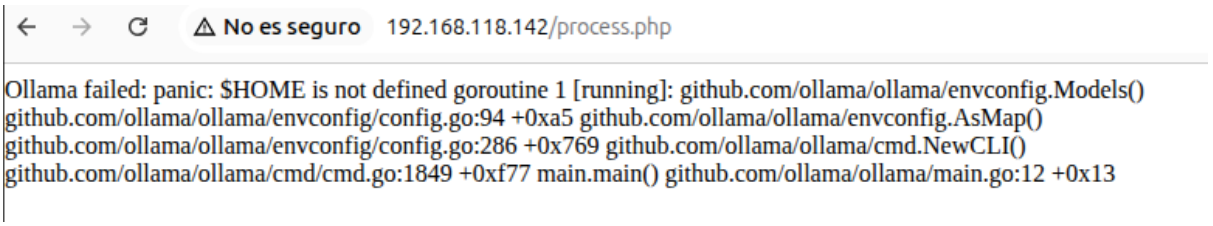
Siga los siguientes pasos en la página web:

1. Abra Aletheia en su navegador.
2. Cargue el archivo: auth.log.
3. Seleccione el modo: Auditoría.
4. Descripción: Revisión de los accesos SSH en el sistema.
5. Haga clic en Subir y analizar



Después de la carga, la página web muestra el siguiente contenido:
Ollama failed: panic: $HOME is not defined goroutine 1 [running]:
github.com/ollama/ollama/envconfig.Models()
github.com/ollama/ollama/envconfig/config.go:94 +0xa5
github.com/ollama/ollama/envconfig.AsMap()
github.com/ollama/ollama/envconfig/config.go:286 +0x769

github.com/ollama/ollama/cmd.NewCLI() github.com/ollama/ollama/cmd/cmd.go:1849 +0xf77 main.main() github.com/ollama/ollama/main.go:12 +0x13



Esto ocurre porque al invocar Ollama en un entorno web, el usuario que ejecuta el servicio (www-data) carece de una variable de entorno HOME definida. En consecuencia, Ollama no puede determinar la ruta de almacenamiento del modelo, lo que provoca un fallo. Debemos resolver este problema configurando explícitamente HOME para este usuario y especificando un directorio seguro.

Crea un directorio HOME específico para Ollama.

- sudo mkdir -p /var/lib/ollama
- sudo chown -R www-data:www-data /var/lib/ollama

```
ub@forense-ai:~$ sudo mkdir -p /var/lib/ollama
[sudo] contraseña para ub:
ub@forense-ai:~$ sudo chown -R www-data:www-data /var/lib/ollama
```

Comprueba si www-data puede usar HOME.

- sudo -u www-data HOME=/var/lib/ollama ollama list

```
ub@forense-ai:~$ sudo -u www-data HOME=/var/lib/ollama ollama list
NAME            ID              SIZE      MODIFIED
phi3:latest     4f2222927938    2.2 GB    44 hours ago
```

Dentro de process.php:

- sudo nano /var/www/forense-ai/process.php

```
ub@forense-ai:~$ sudo nano /var/www/forense-ai/process.php
```

Encontramos esta línea
$cmd = "ollama run " . escapeshellarg($model) . " " . escapeshellarg($prompt);

```
// Llamar a Ollama
$model = "phi3";
$cmd = "ollama run " . escapeshellarg($model) . " " . escapeshellarg($prompt);
```

Reemplácelo por lo siguiente:
$cmd = "HOME=/var/lib/ollama ollama run phi3 " . escapeshellarg($prompt);

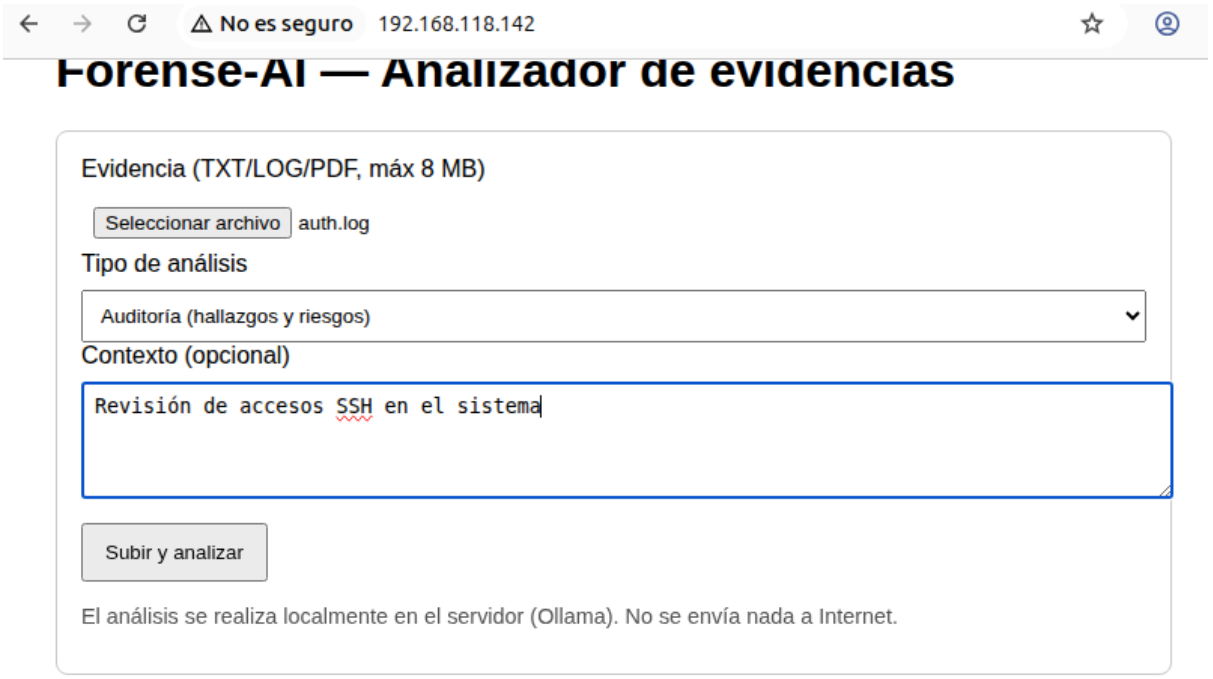
```
// Llamar a Ollama
$model = "phi3";
$cmd = "HOME=/var/lib/ollama ollama run phi3 " . escapeshellarg($prompt);
```

Reiniciar Apache

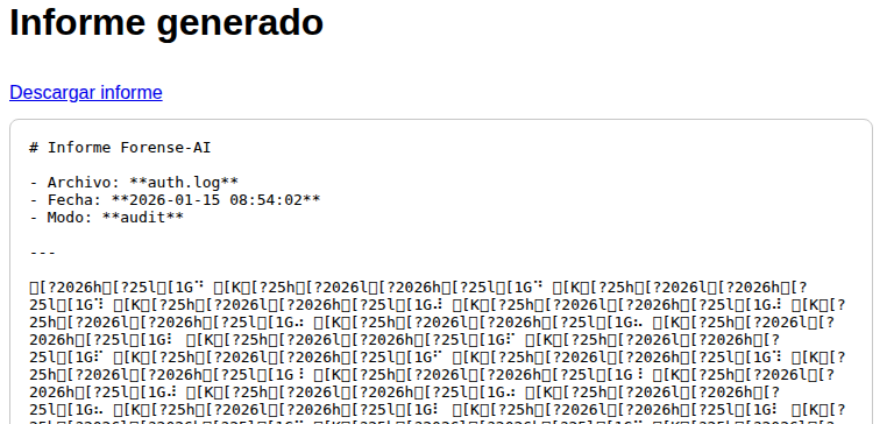
- sudo systemctl reload apache2

```
ub@forense-ai:~$ sudo systemctl reload apache2
```

A continuación, repita la operación en la página web:



Si la página web muestra el siguiente contenido después de la carga, significa que se ha realizado correctamente:



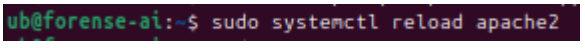
Sin embargo, pueden aparecer caracteres ilegibles. Podemos sustituir toda la sección //Llamar a Ollama por el siguiente segmento:

```
// Llamar a Ollama
$payload = json_encode([
  "model" => "phi3",
  "prompt" => $prompt,
  "stream" => false
]);
```

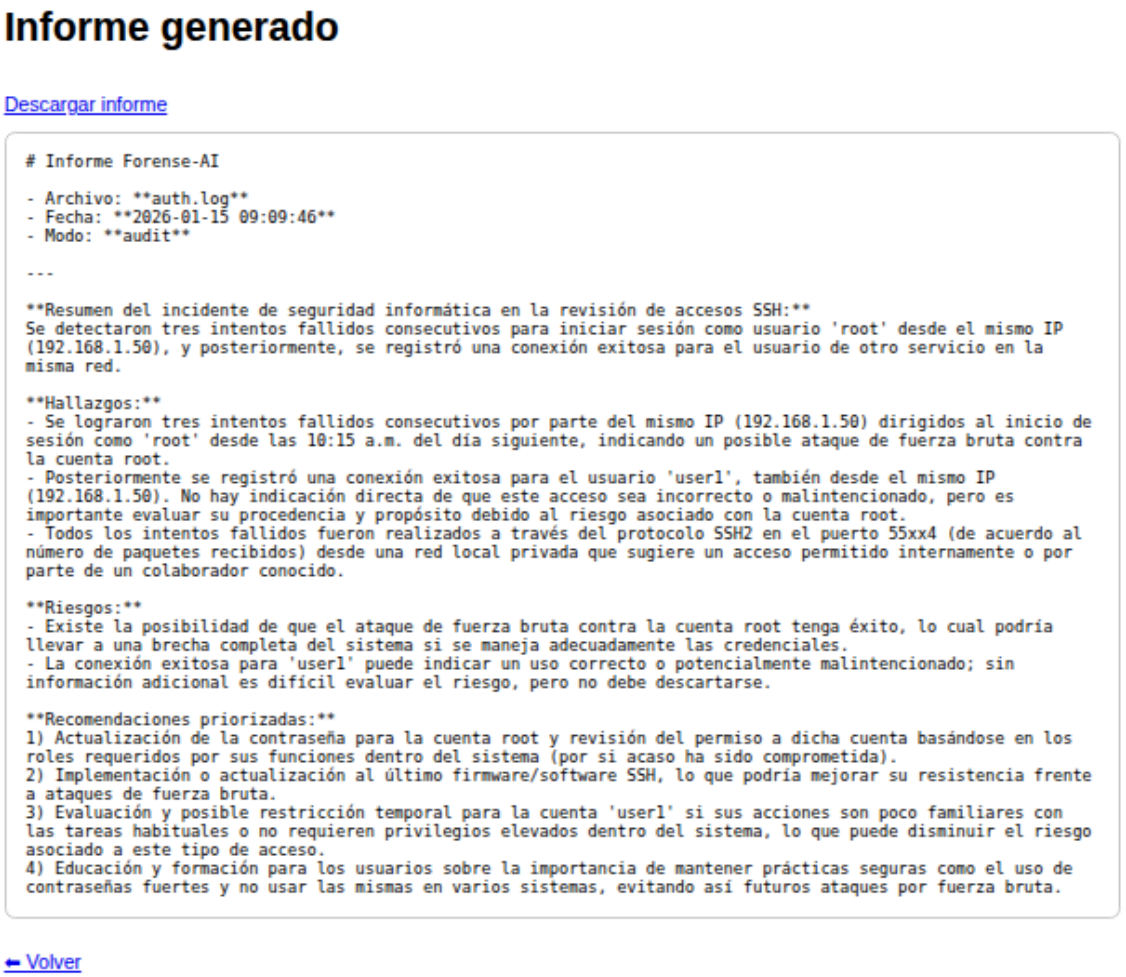
```
$ch = curl_init("http://localhost:11434/api/generate");
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_HTTPHEADER, ["Content-Type: application/json"]);
curl_setopt($ch, CURLOPT_POSTFIELDS, $payload);

$response = curl_exec($ch);
if ($response === false) {
  http_response_code(500);
  exit("Ollama API failed: " . curl_error($ch));
}
curl_close($ch);

$data = json_decode($response, true);
$analysis = $data["response"] ?? "Error: sin respuesta del modelo";

$reportName = basename($dest) . "_informe.md";
$reportPath = $resultDir . $reportName;

$report = "# Informe Forense-AI\n\n"
        . "- Archivo: **" . htmlspecialchars($original) . "**\n"
        . "- Fecha: **" . date("Y-m-d H:i:s") . "**\n"
        . "- Modo: **" . htmlspecialchars($mode) . "**\n\n"
        . "---\n\n"
        . $analysis . "\n";

file_put_contents($reportPath, $report);
```

Reiniciar Apache2

- sudo systemctl reload apache2



Repita el procedimiento en la página web y esta vez, no aparecerá ningún texto ilegible.



2. Caso de prueba B (Forense)

a. Sube una salida de guardada como TXTnmap
b. Modo: Forense
c. Debe generar hipótesis y próximos pasos

Prepare los archivos de prueba (nmap)

- sudo nano 12tmp/nmap.txt

```
ub@ub:~$ sudo nano 12tmp/nmap.txt
```

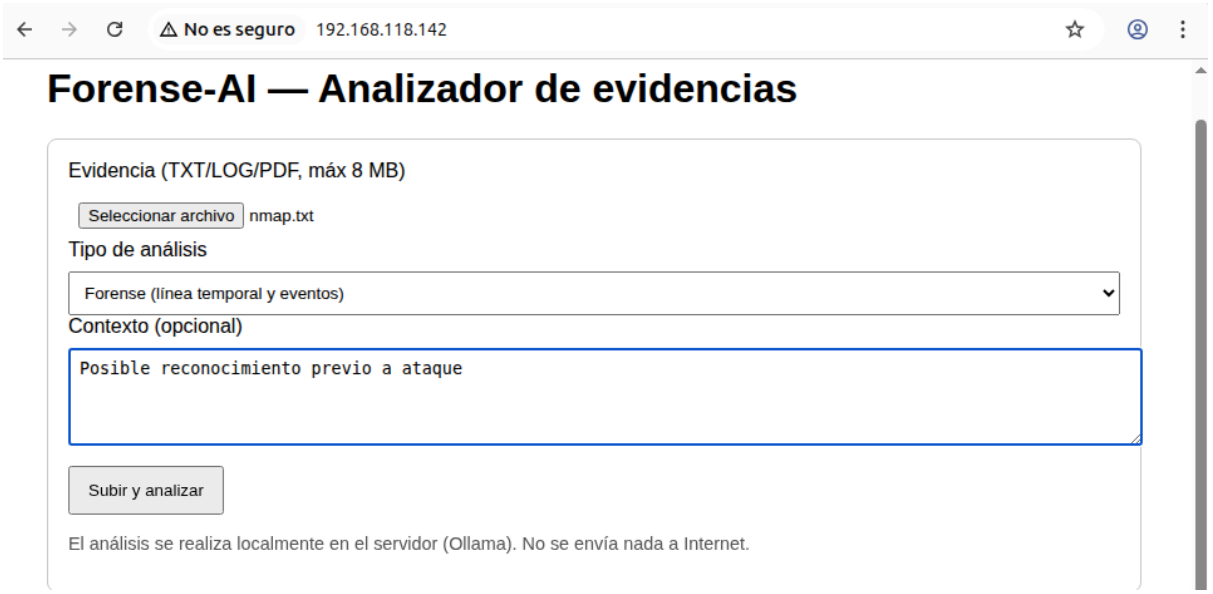
Contenido:

Starting Nmap 7.93 (https://nmap.org) at 2025-01-10 10:30
Nmap scan report for 192.168.1.10
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
3306/tcp open mysql
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds

```
  GNU nano 7.2                          12tmp/nmap.txt *
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-10 10:30
Nmap scan report for 192.168.1.10
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

Operaciones de la página web:

1. Cargar: nmap.txt
2. Modo: Forense
3. Descripción: Posible reconocimiento previo al ataque
4. Haga clic en Subir y analizar



Una vez completada la carga, la página web mostrará el siguiente contenido:

Informe generado

Descargar informe

```
# Informe Forense-AI

- Archivo: **nmap.txt**
- Fecha: **2026-01-15 09:18:07**
- Modo: **forensic**

---

Resumen: El análisis indica que el equipo de red objetivo fue probado previamente, como evidencia por la
detección exitosa del estado operativo en múltiples puertos clave utilizados para comunicaciones y servicios.
Es probable que una persona o grupo con conocimientos técninfluidos haya realizado un reconocimiento previo a
su posible ataque futuro.

Línea temporal aproximada: El informe de enlace fue generado el 10 de enero del año actual, por lo tanto la
actividad detectada es contemporánea al momento exacto indicado (2025), aunque los datos sugieren un evento
pasado reciente o próxima.

Eventos relevantes: La detección abierta en el puerto SSH y servicio web HTTP/HTTPS, junto con MySQL que tiene
estado operativo pero no se está utilizando activamente (puerto 3306), son eventos críticos para la
infraestructura informática. Esto podría indicar una configuración de red vulnerable o posibles puntos débiles
que un atacante potencial buscaría explotar en futuras intrusiones cibernéticas.

Hipótesis: La detección exitosa del estado operativo no abierta para puertos críticos como SSH (22/tcp) y
MySQL sugiere una preparación previa al ataque, posiblemente con la intención de establecer un punto dentro
del sistema para escapar a él más adelante. El hecho que otros servicios web tengan abiertos no necesariamente
implica actividad maliciosa; podría ser por cualquier razón legítima o como distracción durante una intrusión
potencial futura.

Próximos pasos: Se recomienda realizar un análisis de registro más detallado para identificar patrones
sospechosos, actividad forzada en puertas y comandos administrativos no autorizados que podrían haber ocurrido
durante la intrusión. También es aconsejable revisar los permisos de acceso a las cuentas del sistema para
certificar su corrección e integridad, así como actualizar el software y parches críticos ante posibles
vulnerabilidades conocidas que podrían ser explotadas por un atacante. Además, se debe implementar una medida
más robusta de detección de anomalías en la red para identificar futuras intrusiones con mayor precisión y
rapidez.
```

← Volver

3. Caso de prueba C (PDF)

a. Sube un PDF técnico (manual, informe)
b. Modo: Resumen ejecutivo
c. Debe resumir y extraer puntos clave

1. Subir PDF
2. Formato: Resumen ejecutivo
3. Descripción: Documento para la tarea 12
4. Haga clic en Subir y analizar

Forense-AI — Analizador de evidencias

Evidencia (TXT/LOG/PDF, máx 8 MB)

Seleccionar archivo 12_Aletheia.pdf

Tipo de análisis

Resumen ejecutivo

Contexto (opcional)

Documento para tarea 12

Subir y analizar

El análisis se realiza localmente en el servidor (Ollama). No se envía nada a Internet.

El siguiente mensaje indica que la operación se ha realizado correctamente:

Informe generado

Descargar informe

```
# Informe Forense-AI

- Archivo: **12_Aletheia.pdf**
- Fecha: **2026-01-15 09:59:04**
- Modo: **summary**

---

# Resumen Ejecutivo para un responsable no técnico sobre el proyecto Aletheia:
El documento proporciona información detallada acerca del proyecto "Aletheia", que tiene como objetivo la creación de una solución automatizada y segura para analizar evidencias en entornos profesionales. El sistema, llamado servidor Aletheia, se enfoca únicamente en transformar datos técnicos en información estructurada utilizando un motor local inteligente que ayuda a tomar decisiones concretas sobre la situación investigada.

# 5 Puntos Clave:
1. **Seguridad y Control**: Aletheia ofrece una solución más segura al mantener todos los datos procesados dentro del propio servidor, evitando así el envío de información a terceras partes y reduciendo la dependencia en conexiones externas para acceder a recursos.

2. **Desarrollo Educativo**: Este proyecto es una iniciativa educativa que permite alumnos especializados planifican, diseñan y despliegan un servicio capaz de procesar evidencias técnicas en seguridad digital eficiente desde su propio entorno.

3. **Análisis Técnico**: El sistema puede recibir archivos técnicos para análisis, ya sea por auditoría o forense. A través de un motor inteligente localizado, transforma los datos en información estructurada y coherentes que facilita la toma de decisiones basadas en hechos objetivos.

4. **Integración con Procesos Técnicos**: El proyecto no solo analiza evidencias sino también se integra dentro del flujo de trabajo profesional, generando informes claros y reutilizables que pueden aportar al conocimiento técnico actualizado sobre cualquier incidente o auditoría realizada.

5. **Contribución a la Ciberseguridad**: Aletheia busca potenciar las capacidades de ciberseguridad profesional, ayudando en el análisis detallado y comprensivo de evidencias técnicas dentro del contexto de auditoría digital.
```

⬅ Volver