# Vulnyx - Basic


# Informe de Penetración - Laboratorio

**Cliente / Proyecto:** Vulnyx / Basic
**Fecha:** 04/09/2025
**Pentester:** Rubo
**Objetivo:** Evaluación de seguridad en entorno controlado para prácticas de explotación.

## 1. Resumen Ejecutivo

Durante la prueba de penetración al laboratorio **Vulnyx Basic**, se consiguió:

- **Acceso inicial** al servicio SSH mediante un ataque de fuerza bruta sobre el usuario `dimitri`.
- **Escalada de privilegios a root** explotando un binario con permisos SUID ( `env` ).
- **Sin pivoting** a otras redes internas.

  **Impacto simulado**: compromiso total del servidor Linux, con capacidad de ejecutar comandos como administrador y acceso a información sensible.

## 2. Alcance y Metodología

**Alcance:**

- Dirección IP: `192.168.1.129`

- Sistema Operativo detectado: Linux
- Servicios expuestos: `22/tcp SSH`, `80/tcp HTTP`, `631/tcp CUPS`

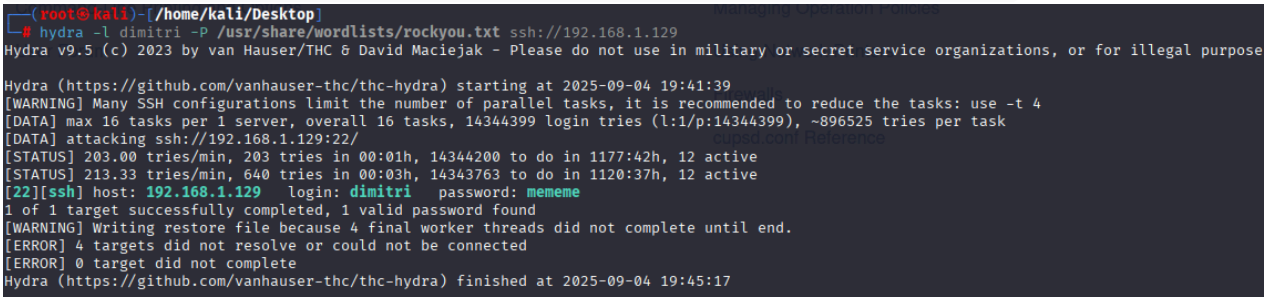
**Metodología (basada en PTES/OSSTMM):**

1. **Reconocimiento** → `arp-scan`, `nmap`
2. **Enumeración** → `dirb`, `gobuster`, `dirsearch`
3. **Explotación** → `hydra` (fuerza bruta SSH)
4. **Post-explotación** → Escalada de privilegios con `env` (GTFOBins)

# 3. Hallazgos Técnicos

## 3.1 Servicio SSH – Ataque de Fuerza Bruta

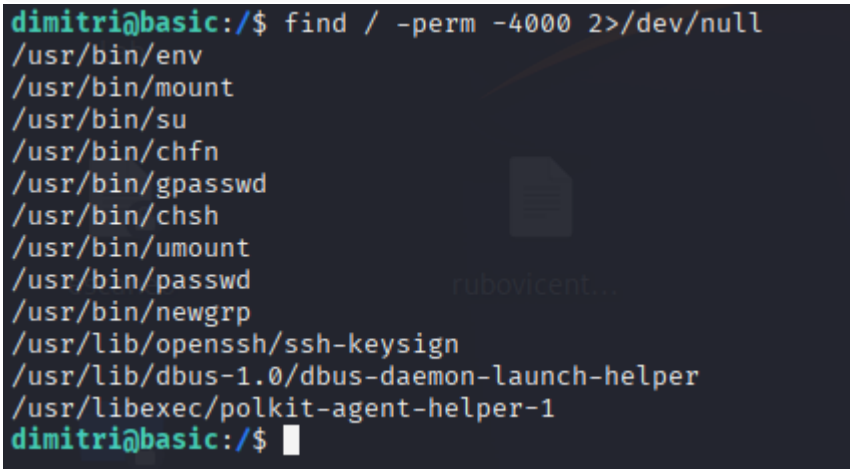
- **Severidad:** Alta
- **Evidencia:**
  `hydra -l dimitri -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.129`
  `[22][ssh] host: 192.168.1.129 login: dimitri password: mememe`




- **Impacto:** Permite acceso remoto al sistema como usuario válido.
- **Recomendación:** Implementar protección contra fuerza bruta (fail2ban, rate limiting), usar contraseñas robustas y autenticación multifactor.

## 3.2 Binario SUID `/usr/bin/env` – Escalada de Privilegios

- **Severidad:** Crítica
- **Evidencia:**
  `find / -perm -4000 2>/dev/null /usr/bin/env ./usr/bin/env /bin/sh -p # id`
  `uid=0(root) gid=0(root) groups=0(root)`



- **Impacto:** Ejecución de comandos como root, control total del sistema.
- **Recomendación:** Revisar y eliminar permisos SUID innecesarios en binarios.

# 4. Impacto en el Negocio (adaptado al laboratorio)

- **Crítico:** Acceso remoto total al sistema como root.
- **Alto:** Compromiso de credenciales de usuario SSH.
- **Medio:** Riesgo de explotación de otros servicios (HTTP, CUPS).

# 5. Recomendaciones Globales

1. Aplicar políticas de contraseñas robustas y rotación periódica.
2. Implementar mecanismos anti-fuerza bruta (fail2ban, bloqueo de IPs).
3. Revisar periódicamente binarios con permisos SUID.
4. Limitar la exposición de servicios innecesarios (ej. CUPS).
5. Aplicar hardening en el servicio SSH (MFA, deshabilitar root login).

# 6. Conclusión

El atacante consiguió acceso a la máquina mediante un ataque de **fuerza bruta SSH** contra el usuario `dimitri`. Posteriormente, se detectó un binario con permisos inseguros ( `env` ) que permitió la **escalada de privilegios a root**.

**Camino seguido:** Reconocimiento y fuzzingweb→ Fuerza Bruta SSH → Acceso inicial como `dimitri` → Escalada con SUID `env` → Root.
**Resultados:** Se demostró que una contraseña débil y la presencia de binarios SUID inseguros permiten comprometer totalmente el sistema.

# *Tabla de Severidades

| Vulnerabilidad | Servicio | Severidad | Impacto |
|---|---|---|---|
| Fuerza bruta SSH | SSH (22) | Alta | Acceso remoto como usuario válido |
| SUID `env` inseguro | Linux | Crítica | Escalada de privilegios a root |
| Exposición CUPS | HTTP (631) | Media | Riesgo de enumeración de usuarios/servicios |