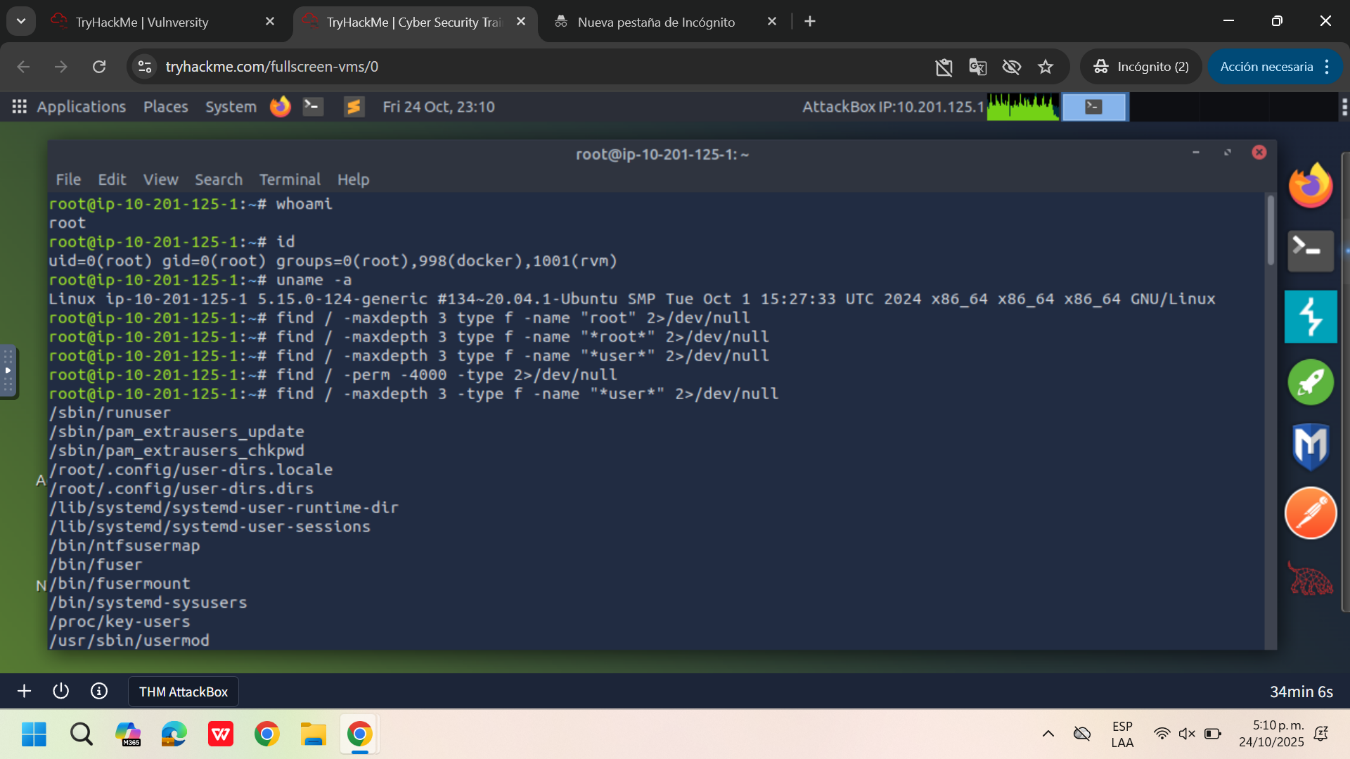
**Pentest básico – Vulnversity (TryHackMe)**

**Integrantes:**

* Diego Borges Rol A
* Maikol Balaguera Rol B

**IP y captura:**



**Resumen ejecutivo**

Se llevó a cabo una prueba de intrusión básica sobre la máquina Vulnversity de TryHackMe con el objetivo de conseguir una shell en nivel de usuario, realizar tareas elementales de post-explotación y recopilar evidencias para el informe. La fase de reconocimiento permitió identificar servicios web y otros servicios de red con posibles debilidades que facilitaron el acceso al sistema a través de vectores relacionados con la aplicación web.

**Hallazgos**

 Servicio HTTP accesible en la IP objetivo, cuyas cabeceras sugieren que el software o versiones instaladas podrían ser vulnerables.

 Se localizaron directorios y recursos web mediante fuerza bruta de rutas (herramientas tipo gobuster), algunos de los cuales contienen información sensible.

 Se detectaron huellas de un servicio Samba/SMB (salida de enum4linux) que podría albergar ficheros o credenciales expuestas.

 Vectores evaluados: inyección de comandos/RCE en endpoints web detectados; enumeración de servicios y búsqueda de pruebas de concepto con searchsploit.**Evidencias**

 thm\_spawn.png (captura de la instancia)

 nmap\_full\_initial.txt (escaneo nmap completo)

 nmap\_service\_enum.txt (detalles de versiones y servicios)

 enum4linux\_output.txt (salida de enumeración SMB)

 fase1\_resumen.txt

 commands\_ran.txt (comandos ejecutados y propósito)

 fase2\_resumen.txt

 equipo.txt (integrantes y roles)

 screenshot\_shell.png (captura mostrando acceso shell)**Recomendaciones**

** Actualizar y parchear los componentes expuestos (servidor web y módulos asociados) a versiones con soporte; revisar CVE relevantes e implementar correcciones críticas sin demora.**

** Reducir la información divulgada por los servicios: ocultar o restringir banners que muestran versiones, deshabilitar módulos o directorios innecesarios y proteger endpoints públicos con reglas (WAF) o controles adecuados.**

** Reforzar el control de acceso: revisar configuraciones de SMB y sudo, eliminar archivos sensibles accesibles desde el webroot, proteger credenciales y aplicar el principio de mínimo privilegio para cuentas y servicios.**