# Reporte de Hallazgos: Laboratorio de Hacking Ético

## 1. Resumen Ejecutivo

Se realizó una prueba de penetración en un entorno virtual de Windows 11 para identificar vulnerabilidades y demostrar la importancia de las defensas. Se logró el acceso al sistema y se estableció una puerta trasera para mantener la persistencia. Se recomienda encarecidamente mantener el sistema y el software actualizados.

## 2. Hallazgos

- \*\*Vulnerabilidad de Explotación:\*\* El sistema fue vulnerable a un ataque del lado del cliente que permitió la ejecución de un payload de Metasploit.

- \*\*Puertos Abiertos:\*\* Se detectaron puertos de SMB (135, 139, 445) activos, que fueron el vector inicial de reconocimiento.

- \*\*Acceso Persistente:\*\* Se instaló con éxito una puerta trasera en la máquina, lo que permitió un acceso continuo al sistema.

## 3. Recomendaciones

1. \*\*Concienciación del Usuario:\*\* Educar a los usuarios para que no ejecuten archivos de origen desconocido.

2. \*\*Mantener el Antivirus Activo:\*\* El antivirus detectó y neutralizó la puerta trasera, validando su eficacia. Se recomienda no desactivarlo.

3. \*\*Mantener el Sistema Operativo Actualizado:\*\* Asegurarse de que el sistema operativo y todas las aplicaciones tengan los últimos parches de seguridad.