Informe Executivo

17 de setembro do 2025

Índice

1 Resumo Executivo

Este informe analiza os riscos dunha máquina de prácticas chamada **Metasploitable 3**, empregada para formación en seguridade informática. Durante a revisión detectouse un fallo moi grave que permitiría a calquera persoa allea **entrar no sistema sen permiso e tomar o control completo**.

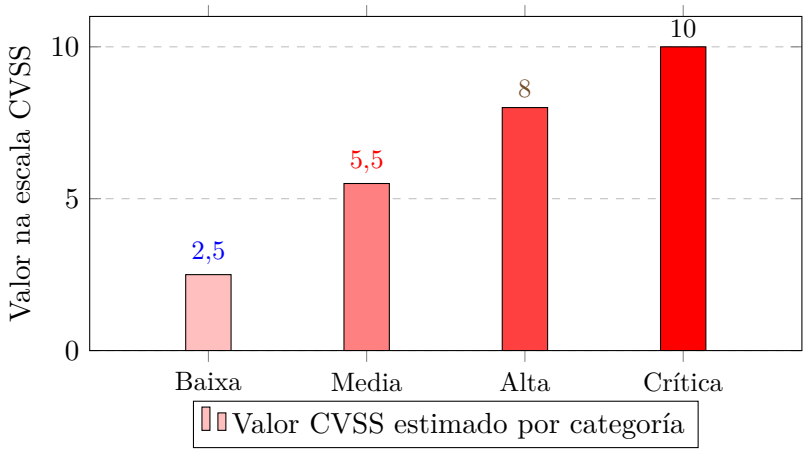
A gravidade desta vulnerabilidade é alta. Se un sistema con este tipo de erro estivese conectado á rede da empresa, **podería poñer en perigo datos confidenciais, interromper o funcionamento normal e causar perdas económicas importantes**.

Este tipo de situación representa unha ameaza seria para calquera organización, polo que é fundamental limitar o uso desta máquina a contornos pechados e controlados, exclusivamente con fins educativos.

2 Escala de Gravidade das Fallas (CVSS)

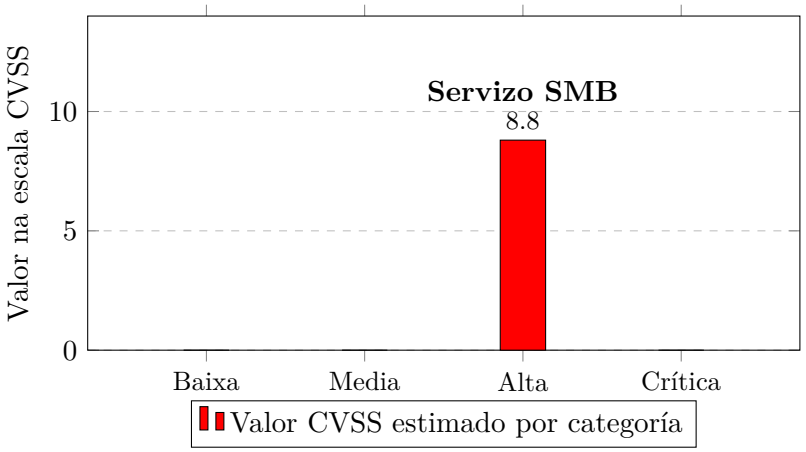
As fallas de seguridade clasifícanse segundo o seu nivel de gravidade mediante un sistema internacional chamado CVSS:

- **Baixa (0.0 – 3.9)**: poucos efectos ou difíciles de aproveitar.
- **Media (4.0 – 6.9)**: poden causar problemas pero teñen limitacións.
- **Alta (7.0 – 8.9)**: poden ser aproveitadas con certo impacto.
- **Crítica (9.0 – 10.0)**: moi fáciles de usar e con consecuencias graves.



3 Vulnerabilidade crítica detectada: Impacto moi grave

Detectouse unha falla moi coñecida no servizo de compartición de ficheiros (SMB), cunha puntuación **CVSS: 8.8**. Esta falla permitiría a unha persoa allea controlar o sistema remotamente sen permiso.



4 Consecuencias para a organización

IMPACTO CRÍTICO NOS ACTIVOS E NAS FINANZAS DA EMPRESA

Unha vulnerabilidade alta pode derivar nun impacto empresarial moi relevante. A exposición de activos tecnolóxicos —como servidores, datos ou redes internas— pode provocar interrupcións operativas, acceso non autorizado a información sensible e, sobre todo, **perdas económicas significativas** para a organización.

Impacto interno

- Acceso non autorizado á información interna.
- Posibilidade de alterar ou borrar documentos importantes.
- Acceso a outras partes da rede da empresa sen permiso.
- Interrupción do funcionamento normal dos sistemas.

Impacto externo

- Filtración de datos de clientes ou colaboradores.
- Uso da infraestrutura da empresa para actividades ilícitas.
- Perda de confianza da clientela e dano á imaxe pública.
- Posibles perdas económicas por interrupción do servizo, restauración de sistemas ou sancións legais derivadas do incumprimento normativo.
- Posibles sancións legais se hai incumprimento normativo.

Ricardo Feijoo Costa

5 Recomendacións

- Esta máquina debe utilizarse **só en contornos controlados** e desconectados da rede principal.
- O uso debe ser supervisado por persoal especializado en formación.
- É recomendable informar aos usuarios dos riscos antes das prácticas.
- Nunca debe reutilizarse esta imaxe en contornos reais de traballo.
- Manter sempre actualizados os sistemas operativos, aplicacións e servizos para reducir riscos coñecidos.

Ricardo Feijoo Costa