Samuel Cordero
Dervis Martinez V - 31.456.326

Conclusión

Este pequeño proyecto de PC demuestra cómo, con un presupuesto de menos de $2500, se puede armar una estación de trabajo increíblemente capaz para ciberseguridad y hacking ético. En este ámbito, al igual que en las simulaciones de inteligencia artificial, las pruebas de intrusión y los análisis de vulnerabilidades requieren una potencia de procesamiento superior, disponibilidad constante y análisis en tiempo real.

Por eso, decidimos construir la computadora desde cero, eligiendo cada pieza con precisión para satisfacer las necesidades profesionales. El resultado es una máquina que puede funcionar **24/7** sin interrupciones, actuando como un laboratorio digital automatizado y autónomo. Este entorno controlado es clave para realizar pruebas de penetración, análisis forense, simular redes vulnerables, usar sandboxes para malware y trabajar con herramientas avanzadas como Metasploit, Wireshark y Burp Suite. El objetivo principal es crear escenarios realistas de ataque y defensa, analizar los resultados, registrarlos y aprender de ellos para mejorar las estrategias de ciberdefensa.

Dada la alta demanda de procesamiento de datos, análisis en tiempo real y la necesidad de manejar múltiples máquinas virtuales y contenedores, los componentes seleccionados debían garantizar un rendimiento superior y una estabilidad duradera. Una computadora prefabricada simplemente no podría ofrecer la optimización necesaria para estas tareas tan específicas. Por lo tanto, armar un equipo personalizado fue la mejor opción para cumplir con los altos estándares profesionales de esta disciplina. Este enfoque asegura un ambiente de trabajo confiable, escalable y seguro, esencial para estudiar y aplicar habilidades de hacking ético, fortaleciendo así la protección de sistemas reales contra las amenazas emergentes.