Samuel Cordero V-31.678.592
Dervis Martinez V-31.456.326

Universidad de Carabobo
Facultad de Ciencias y Tecnología
Departamento de Computación
Arquitectura del Computador

Argumento

En el ámbito de la ciberseguridad, particularmente en el área del hacking ético, contar con una estación de trabajo robusta y especializada es fundamental. Al igual que en simulaciones complejas de inteligencia artificial, los entornos de prueba que se requieren para prácticas éticas de intrusión, análisis de vulnerabilidades y simulación de ataques cibernéticos también demandan un alto poder de procesamiento, disponibilidad continua y capacidad de análisis en tiempo real.

Por esta razón, se opta por ensamblar un computador desde cero, eligiendo cuidadosamente cada componente según las necesidades específicas del uso profesional. Esta máquina está diseñada para operar 24/7 sin interrupciones, funcionando como un entorno controlado donde se realizarán pruebas de penetración, análisis forense digital, simulaciones de redes vulnerables, entornos de malware sandboxing y pruebas con herramientas de explotación como Metasploit, Wireshark, Burp Suite, entre otras.

El objetivo principal es crear un laboratorio digital autosuficiente y automatizado, que permita evaluar cómo sistemas reales y artificiales reaccionan ante ataques o amenazas preestablecidas, todo dentro de los marcos legales y éticos que rigen al hacker ético. Se requiere de un sistema que no solo genere escenarios realistas y variados de ataque/defensa, sino que también los analice, registre y aprenda de cada resultado para mejorar estrategias de ciberdefensa.

Debido a la naturaleza intensiva en datos, análisis en tiempo real y necesidades de virtualización y contenedores, los componentes seleccionados deben ofrecer un rendimiento superior y estabilidad prolongada. Optar por una computadora prefabricada limitaría la optimización necesaria para estas tareas tan específicas. Por tanto, construir un equipo personalizado es la mejor opción para cumplir con los estándares profesionales que esta rama requiere.

Este enfoque garantiza un entorno confiable, escalable y seguro para el estudio y aplicación de las habilidades propias del hacking ético, con el fin de fortalecer la defensa de sistemas reales ante amenazas emergentes.

Para los profesionales de la ciberseguridad y el hacking ético, una estación de trabajo **potente y específica** es indispensable. Al igual que en la inteligencia artificial, las pruebas de intrusión, el análisis de vulnerabilidades y la simulación de ataques cibernéticos requieren un **alto rendimiento computacional**, disponibilidad constante y capacidad de análisis en tiempo real

Dadas las intensas demandas de procesamiento de datos, análisis en tiempo real y la necesidad de virtualización y contenedores, los componentes elegidos deben garantizar un **rendimiento superior y estabilidad**. Las computadoras prefabricadas no ofrecen la optimización necesaria para estas tareas especializadas. Por tanto, construir un equipo personalizado es la solución óptima para cumplir con los estándares profesionales de esta disciplina.