**PRÁCTICA N°3**

**TEMA: “ANALISIS DE MALWARE EN UN AMBIENTE SANDBOX”**

**1. OBJETIVOS**

1.1 Configurar un ambiente controlado de pruebas (Sandbox).

1.2 Analizar el tráfico de malware con Wireshark.

1.3

**2. PREPARATORIO**

2.1 ¿Consultar que es un análisis de malware y cuales con sus objetivos?

2.2 ¿Investigue sobre el sandbox?

2.3 ¿Realizar un cuadro resumen sobre la herramienta de Wireshark? ¿Cómo identifica el tráfico malicioso?

**3. PRACTICA**

**4. INFORME**

4.1 Enumerar los cambios observados en los procesos del sistema tras ejecución del malware?

4.2 ¿Al detectar el trafico sospechoso con Wireshark, se identificó un patrón? Describir el patrón y el destino.

4.3 Cuales son las medidas de prevención en este tipo de malware en un entorno real?

**5. REFERENCIAS BIBLIOGRAFICAS**