**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.

**3. REACTIVOS**

¿Qué es un ataque de ARP Spoofing?

1. Un ataque que desactiva las tablas ARP de los dispositivos
2. Un ataque donde el atacante envía respuestas ARP falsas para redirigir en el tráfico de red.
3. Un ataque que bloquea el acceso a los servidores DNS.
4. Un ataque que utiliza malware para cifrar archivos en un sistema.

¿Qué tipo de paquetes se debe buscar en Wireshark para detectar ARP Spoofing?

1. Paquetes DNS
2. Paquetes TCP
3. Paquetes ARP
4. Paquetes ICM

¿ Medidas que pueden prevenir un ataque de ARP Spoofing?

1. Utilizar autenticación ARP.
2. Implementar un firewall personal.
3. Usar un software de detección de intrusiones.
4. Configurar VPN en todos los dispositivos.