**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.

**5. INFORME**

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

Luego de ejecutar el ataque de ARP Spoofing se identifican los siguientes cambios en el sistema:

1. **Alteración de las tablas ARP**

Las tablas ARP en la maquina víctima se modifican, es decir, las direcciones IP de Gateway y la dirección MAC están vinculadas a las direcciones del atacante.

1. **Interrupción o redirección del Trafico de la red**.

Algunos servicios y aplicaciones dependientes de la conectividad de la red muestran fallas o desempeños anómalos debido al tráfico interceptado por el atacante.

1. **Incremento de Trafico de Red Sospechoso**

Incremento en los mensajes ARP, especialmente en la peticiones repetitivas o respuestas no solicitadas.

***5.2 ¿Al detectar el tráfico sospechoso con Wireshark, se identificó un patrón? Describir el patrón y el destino.***

El patrón del trafico detectado es la presencia de múltiples ARP probes dirigidas a Broadcast (ff:ff:ff:ff:ff:ff) preguntando Who has para la dirección IP 192.168.1.2.

Las respuestas falsas están diseñadas para engañar a los dispositivos como la victima o el Gateway.

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

* Implementar seguridades en Switch para inspeccionar los paquetes ARP y permitir el ingreso solo aquellos que coincidan con las entradas de DHCP.
* Segmentar las redes y VLans para tener una limitación de la propagación de ARP.
* Utilizar protocolos de red seguro como HTTPS, SSH, VPN.
* Monitoreo constante del trafico de red para identificar actividad sospechosa.