**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.

**2. PREPARATORIO**

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

El análisis de malware es proceso que permite examinar software malicioso para poder entender el funcionamiento y mitigar el riesgo. El análisis es importante para proteger los sistemas y redes ante amenazas cibernéticas.

El objetivo de este análisis es identificar el tipo de malware, estudiar el comportamiento en el sistema, ver el impacto que causa en el sistema, detener el malware y prevenir el sistema pata evitar que este sea infectado por malware [1].

***2.2 ¿Investigue sobre el sandbox?***

Un Sandbox o conocido como ambiente de aislado el cual permite realizar pruebas de penetración de malware para poder observar el comportamiento del malware sin causar daños al sistema [2].

El ambiente controlado permite analizar los daños causado al sistema que se encuentra dentro de él, para poder encontrar correcciones y mitigar este malware [2].

***2.3 ¿Qué es una tabla ARP t para que sirve?***

Las tablas ARP son bases de datos que se almacena en dispositivos de red como Router, computadoras los cuales mapean las direcciones IP a sus correspondientes direcciones MAC [3].

La tablas ARP son útiles porque la dirección de software del host conectado a la red debe traducirse a una dirección de hardware. Sin un ARP, un host no podría determinar la dirección de hardware de otro host [3].

***2.4 ¿Investigue que es el ARP Spoofing?***

El ARP Spoofing es un ataque en el que el atacante envía mensajes ARP falsos a una red LAN con el objetivo de asociar a la dirección MAC del atacante con la dirección IP de la víctima [4].

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

|  |  |
| --- | --- |
| Características | Descripción |
| Definición | Wireshark es una herramienta que permite analizar protocolos de red capturando paquetes de datos en tiempo real [5]. |
| Funcionalidad | Monitoreo, captura y análisis del trafico de red para diagnosticar problemas y anomalías |
| Formatos de Archivos soportados | Captura de formatos como pcap. pcapng entre otros [5]. |
| Protocolos Soportados | Soporta protocolos de red como TCP, UDP, HTTP, FTP, ARP [5]. |

Wireshark identifica el trafico malicioso mediante el análisis de patrones anómalos en el tráfico de red [6].

Bibliografía

[1] M. Sikorski, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, 1 st. 2012.

[2] M. Egele, T. Scholte, E. Kirda, y C. Kruegel, «A survey on automated dynamic malware-analysis techniques and tools», *ACM Comput. Surv.*, vol. 44, n.o 2, pp. 1-42, feb. 2012, doi: 10.1145/2089125.2089126.

[3] «Qué es el protocolo de resolución de direcciones (ARP)», Fortinet. Accedido: 21 de enero de 2025. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/what-is-arp.html

[4] H. Nasser y M. Hussain, «An Effective Approach to Detect and Prevent ARP Spoofing Attacks on WLAN», *Iraqi J. Electr. Electron. Eng.*, vol. 19, n.o 2, pp. 8-17, dic. 2023, doi: 10.37917/ijeee.19.2.2.

[5] «Wireshark · Go Deep». Accedido: 20 de enero de 2025. [En línea]. Disponible en: https://www.wireshark.org./

[6] L. Chappell y G. Combs, *Wireshark® 101: essential skills for network analysis*, 2nd edition. en Wireshark solution series book. Reno, Nev: Protocol Analysis Institute, Inc, Chappell University, 2017.