FACULTAD DE INGENIERÍA

Carrera Profesional de Ingeniería de Sistemas e Informática

Tarea 2

Amenazas de Red

Curso:

Seguridad Informática

Sección:

31437

Docente:

ENZO RUBEN HEREDIA MELENDEZ

Presentado por:

Cutimbo Jibaja, Daniel Alberto

Arequipa – Perú

2022

Explica con tus propias palabras : ¿Qué son las amenazas de red, metodologías de ataque y protección de la información? Además, brinda ejemplos.

Amenazas de Red:

Las amenazas de red es todo aquello que pueda causar problemas, romper el sistema o vulnerar la seguridad de la información. Pueden ser agrupados en 4 categorías:

- **Malware:** Este es un software creado con código malicioso cuyo objetivo principal es conseguir acceso a los sistemas, robar información y comprometer el funcionamiento habitual de las operaciones del sistema.

  Ejemplos: Uno de los ejemplos más famosos fue el Ransomware WannaCry, que fue lanzado en el 2017, este malware de cifrado encriptaba la información del usuario y solicitaba un pago en Bitcoin por la clave de desencriptación si se quería recuperar la información.

Fuente: https://www.segurosciberriesgos.es/wannacry.html

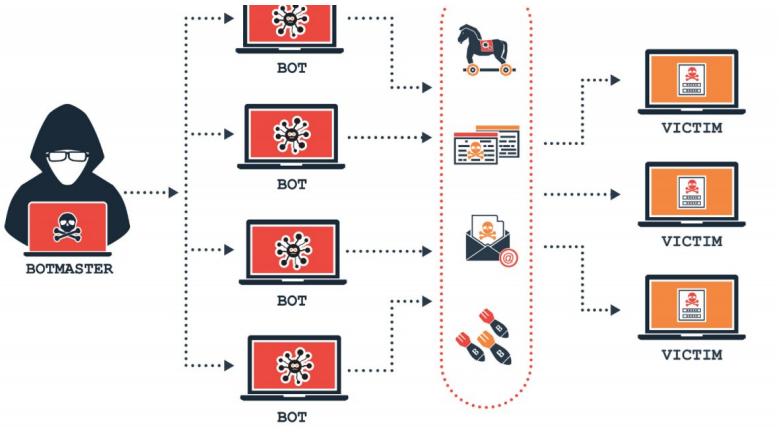
- **Virus:** Este código tiene por objetivo propagarse a la mayor cantidad de sistemas, y esto lo logra replicándose a si mismo por medio de la interacción con el usuario que no conoce su verdadero propósito.

  Ejemplos: Los principales casos en esta categoría son de Spyware, este código se descarga adjunto a un archivo, toma control de un sistema (cámaras, radios, modems, routers, etc) intercepta el tráfico de la red y lo reenvía al atacante.

Fuente: Mr.Robot Season 1 Ep. 2

- **Gusanos:** Este es una variante del virus, su principal diferencia es que no es necesario ningún tipo de intervención para que se auto replique e infecte más sistemas a través de las redes.

  Ejemplos: Esta amenaza al no depender de la interacción directa del usuario, hace que su propagación sea casi indetectable, sobretodo si no se cuenta con un antivirus capaz de detectarlo, este tipo de infección se usa principalmente para crear las famosas botnets, donde un anfitrión posee el control de miles de ordenadores para enviar ataques ddos, spam, y propagar más el gusano.



Fuente: https://www.redseguridad.com/actualidad/cibercrimen/que-es-una-botnet-y-como-puedo-prevenirla-y-evitarla_20210630.html

- **Phishing:** Es un ataque que aplica la ingeniería social, pues hace parecer que su contenido u origen es legítimo para que las víctimas brinden sus datos personales y/o credenciales de acceso.

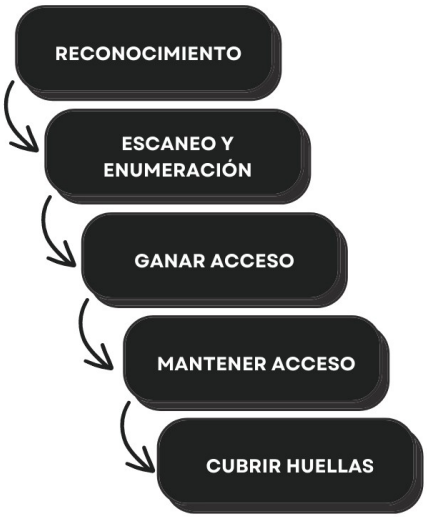
  Ejemplos: Este caso tuvo un mayor impacto recientemente en la comunidad Gamer, constantes enlaces aparecían en los mensajes de amigos en plataformas como Steam y Discord, donde te pedían apoyo para votar por su equipo u

regalos en páginas que te pedían acceder con tu cuenta. De esta forma los atacantes obtenían tus credenciales de acceso y repetian el ciclo con tus demás contactos al reenviar el mensaje sin que te dieras cuenta.

Fuente: https://foro.hermandadfenix.es/t/cuidado-con-scam-en-steam/20126

Metodologías de Ataque:

- **Reconocimiento:** Aquí los atacantes averiguan todo lo posible sobre su objetivo, que sistema usa, sus vulnerabilidades, quienes poseen acceso, etc. Aquí se emplea principalmente la ingeniería social.
- **Escaneo:** Los atacantes acceden a la red de forma remota y monitorizan todo el tráfico para obtener credenciales de acceso, información importante, etc. Aquí el software de Wireshark puede ser utilizado.
- **Acceso:** Los atacantes emplean brechas de seguridad para obtener acceso a la red y al sistema, por medio de los exploits, ataque de diccionario para obtener las contraseñas en base a palabras clave que la víctima suele usar (método más efectivo) o ataques de fuerza bruta que saturan al sistema con muchas contraseñas hasta que se consigue acceder (es el método más lento).
- **Mantener acceso:** Una vez que los atacantes obtienen acceso al sistema, es importante para ellos asegurarse que puedan acceder a él cuando deseen, por ello desarrollan e implementan backdoors o puertas traseras (usando protocolos SSH, rootkid con permisos de administrador) u troyanos.
- **Borrado de huellas:** Lo más importante para los atacantes es no dejar rastros de su actividad para evitar ser descubiertos, para ello usan los rootkid que se ejecutan para brindar acceso y en caso necesario eliminar cualquier rastro de la memoria del dispositivo.



Fuente: https://academy.seguridadcero.com.pe/blog/fases-ethical-hacking

Protección de la Información:

La protección de la información viene siendo presentada en 4 controles establecidos por la ISO 27032, Claúsula 12:

- Controles de nivel de aplicación: Es recomendable realizar pruebas de seguridad habituales para detectar fallos y corregirlos.

- Protección del servidor: Instalación de software anti-malicioso (antivirus), copias de seguridad, evaluaciones de vulnerabilidades y pruebas.

- Controles del usuario final: Aplicaciones de software soportadas, antivirus.

- Controles contra ingeniería social: Educación y capacitación del personal sobre las amenazas y sus métodos de ataque.

- Aplicación de defensa en capas: Esta estrategia se centra en crear barreras de seguridad sobre la información, entre mayor cantidad de capas, más difícil y más tiempo le toma al atacante atravesarlas lo que da tiempo al equipo de ciberseguridad a detectar la incursión no autorizada y tomar medidas defensivas.

Bibliografía:

- Belcic, I. (2019, 28 de septiembre). *La guía esencial del malware: detección, prevención y eliminación*. La guía esencial del malware: detección, prevención y eliminación. https://www.avast.com/es-es/c-malware
- *¿Qué es el ransomware WannaCry?* (s. f.). www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/ransomware-wannacry
- *'Rootkit': definición, tipos y protección ante este 'malware'*. (s. f.). Redseguridad. https://www.redseguridad.com/actualidad/cibercrimen/rootkit-definicion-tipos-y-proteccion-ante-este-malware_20210712.html#:~:text=Un%20rootkit%20es%20un%20paquete,conocimiento%20o%20consentimiento%20del%20usuario.
- *What is a Zero-day Attack? - Definition and Explanation*. (s. f.). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit