UNIVERSIDAD AUTÓNOMA DE ZACATECAS

UNIDAD ACADÉMICA DE INGENIERÍA ELÉCTRICA

PROGRAMA DE INGENIERÍA EN COMPUTACIÓN

SEGURIDAD EN REDES DE COMPUTADORAS

INTRODUCCIÓN A LA CIBERSEGURIDAD

GILBERTO HUERTA REYNOSO
INSTRUCTOR: CARLOS HÉCTOR CASTAÑEDA RAMÍREZ
Zacateas, Zacatecas a 31 de enero del 2023

1. **¿Qué es ciberseguridad?**
   Ciberseguridad, es la aplicación de tecnologías, procesos y controles para proteger sistemas, redes, programas, dispositivos y datos de ciberataques.

2. **¿Cuál es el objetivo de la ciberseguridad?**
   Su objetivo es reducir el riesgo de ciberataques y proteger contra la explotación no autorizada de sistemas, redes y tecnologías.

3. **¿Qué es la triada de la Ciberseguridad?**
   Confidencialidad
   Garantizar que la información es accesible sólo para aquellas personas autorizadas. Por medio de Autenticación y autorización, encripción, borrado remoto, capacitación usuarios.
   Integridad
   Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento y transmisión. Por medio de la Encripción, firmas digitales, certificados digitales, sistemas de detección de intrusos, control de versiones.
   Disponibilidad
   Garantizar que los usuarios autorizados tienen acceso a la información y a los recursos relacionados toda vez que lo requieran. Por medio de la Redundancia de servidores y sus componentes, actualizaciones de software.

4. **¿Qué es Malware?**
   Cualquier código utilizado para robar datos, evitar controles de acceso, ocasionar daños o comprometer un sistema de red y la información.
   Se instala en el sistema cuando el usuario hace clic en un enlace en un correo electrónico, visita sitios web engañosos o descarga archivos sin analizar.
   Algunos tipos:
   - Virus
   - Gusanos
   - Spyware
   - Bot
   - Rootkit
   - Ransomware

5. **¿Qué es el Ransomware?**
   Tipo de malware que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.
   Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.
   El rescate debe pagarse en algún tipo de criptomoneda para evitar el rastreo.
   El método más común de infección es a través de un anexo en un correo electrónico enviado al usuario mediante phising.
   Ejemplos: CryptoLocker, WannaCry, Ryuk, Maze (chacha), Conti(IOPC), Revil (Sodin), Netwalker (MailTo), DoppelPaymer.

6. **¿Qué es el Social Engineering?**

   Intenta manipular a las personas para que realicen acciones, cometan errores de seguridad o divulguen información confidencial.

   Se aprovecha de la disponibilidad de las personas de ayudar, y también se explotan sus debilidades como vanidad, miedo, codicia.

   Se pretender ser otra persona: una autoridad, un empleado, solicitando información de forma inusual o desesperada.

   Puede falsificarse gafetes para acceder a espacios restringidos o entrar detrás de alguien que tiene ese acceso.

   Ponerse tras el teclado para mirar cuando se teclean contraseña, hasta escuchar conversaciones privadas sin autorización.

7. **¿Qué es el Phising?**

   Correos electrónicos malicioso disfrazados como confiables o legítimos.

   Engaña al usuario para que comparta información personal, o haga clic en algún enlace que instala malware, o captura credenciales de acceso.

   En algunos casos viene con faltas de ortografía, malas redacciones o traducciones, además de que el dominio del correo del remitente es algo sospechoso, o al poner el puntero sobre el enlace en el cuerpo del correo, no coincide con lo que dice el texto.

   Puede ser muy difícil de detectar, puede ser en apariencia muy formal y parecerse al de tu banco, empresa de trabajo, tiende de conveniencia, que te pide actualizar tus datos y te envía a un sitio web falso para robar tus datos.

   Puede ser dirigido a empleados específicos de una empresa (spear phisig).

8. **¿Qué es el Zero-day Exploit?**

   Se explota una vulnerabilidad recien descubierta o no reportada.

   No existe aún un parche de seguridad o actualización que la mitigue por parte del fabricante o desarrollador.

   Existe un mercado negro de venta de Zero-day exploits, lo que incremente el riesgo. Suelen ofrecerse en paquete como un software como servicio (software as a service) donde creador recibe parte del beneficio una vez efectuado el ataque, ya sea por la venta o por comisión del pago de rescate en el caso de ransomware.

9. **¿Qué es Denial of Service Attack (DoS)?**

   Inunda los sistemas, redes o servidores con tráfico masivo, lo que hace que el sistema no pueda cumplir con las solicitudes legítimas.

   Puede agotar los recursos de un sistema como memoria, espacio en disco duro.

   Se pueden utilizar varios dispositivos infectados para lanzar un ataque en el sistema objetivo, generando una de denegación de servicio distribuida (DDoS).

   Contenerlo puede ser difícil dado que se falsifican las direcciones IP de origen (IP Spoofing) y puede requerir equipamiento especial, o contramedidas a nivel proveedor de servicios.

10. **¿A qué se refiera el Man in the midle?**

    Ponerse en medio de la comunicación entre dos partes.

    Mediante la escucha y captura de paquetes enviados por la red, se puede tener acceso a datos confidenciales, o incluso modificar la respuesta al usuario.

    Si los datos no viajan cifrados (texto plano) son fácilmente interceptados.

    En algunos casos es posible interceptar datos cifrados y aplicar técnicas de cracking para obtener contraseñas en texto plano (wifi cracking).

11. **¿Qué es el Password cracking?**

    Se prueban diversas contraseñas posibles hasta adivinar la correcta (guessing).

    Se prueban combinaciones numéricas o alfabéticas como contraseñas.

    Se prueban palabras en un diccionario como contraseñas.

    Se prueban combinaciones de palabras de diccionario con frases al inicio o al final de estas palabras.

    Finalmente, como último recurso, se van combinando todos los caracteres posibles en todas las posiciones.

12. **¿A qué se refiere el Covert Hardware?**

    El atacante puede utilizar diferentes dispositivos de hardware que le faciliten la infiltración encubierta en las redes y sistemas.

13. **¿Qué es un Hacker?**

    Personas con amplios conocimientos de informática, exploran diversas técnicas para sobrepasar los controles de seguridad y explotar las vulnerabilidades en redes y sistemas. Desarrollan nuevas técnicas de ataque por la emoción del desafío o para presumir en la comunidad de hackers.

14. **¿Cuáles son los Black Hat Hackers?**

    Operan en el anonimato, motivados por el beneficio personal o económico, la venganza, el acecho o el activismo político.

15. **¿Cuáles son los White Hat Hackers?**

    Operan bajo permiso expreso del dueño de la red o sistema, y al cual le reportan sus los hallazgos como entregable del contrato, también llamados, hackers éticos o analistas de seguridad.

16. **¿Qué hacen los Terrorist groups?**

    Llevan a cabo ataques cibernéticos para destruir, infiltrarse o explotar la infraestructura crítica para amenazar la seguridad nacional, comprometer el equipo militar, perturbar la economía y causar bajas masivas.

    En algunos casos patrocinados por gobiernos con fines de inteligencia / ciber guerra. A veces llamados también grupos APT (Advanced Persistent Threat).

17. ¿Qué son los Malicious Insiders?

Son personas con información privilegiada, pueden incluir empleados, proveedores externos, contratistas u otros socios comerciales.

Tienen acceso legítimo a los activos de la empresa, pero hacen un mal uso para robar o destruir información con fines de lucro personal o financiero.

Atacan por venganza al no ser promocionados, o infiltrados a propósito para filtrar secretos comerciales. Son más difíciles de detectar que los atacantes externos, dado que la organización confía en ellos.