ENERO DE 2024

CONCEPTOS BÁSICOS

TÉCNICAS GENERALES DE ATAQUES 2

CÉSAR ANTONIO

ING. CÉSAR ANTONIO RÍOS OLIVARES
DOCENTE DE ASIGNATURA
WWW.CESARANTONIO.PRO

INTRODUCCIÓN

En el actual panorama digital, la ciberseguridad se ha convertido en una prioridad esencial. Los ataques informáticos representan una amenaza constante para la integridad, confidencialidad y disponibilidad de la información.

Esta reseña abordará los tipos de ataques informáticos, explorando sus conceptos básicos, ejemplos prácticos, casos reales, actividades sugeridas de aprendizaje y conclusiones.

2. Conceptos básicos

Los ataques informáticos abarcan una amplia gama de técnicas maliciosas dirigidas a sistemas informáticos y redes. Estos se clasifican en diversas categorías, incluyendo:

Malware: Software malicioso diseñado para dañar o explotar sistemas, como virus, gusanos, troyanos y ransomware.

Phishing: Intentos de engañar a usuarios para obtener información confidencial, como contraseñas y detalles de cuentas.

Ataques de Denegación de Servicio (DoS): Sobrecarga de recursos de un sistema para impedir su funcionamiento normal.

Inyección de Código: Introducción de código malicioso en aplicaciones para ejecutar comandos no autorizados.

Ataques de Ingeniería Social: Manipulación psicológica de personas para obtener información confidencial o acceso no autorizado.

3. Ejemplos prácticos

3.1. Malware

Ejemplo Práctico: Ransomware "Cryptolock"

El ransomware Cryptolock es un malware que cifra archivos en el sistema de la víctima y exige un rescate para restaurar el acceso. Un usuario podría descargarlo inadvertidamente al abrir un correo electrónico de phishing y hacer clic en un enlace malicioso. Cryptolock encripta los archivos personales del usuario y muestra un mensaje de rescate, solicitando el pago de una suma en criptomonedas para la clave de descifrado.

3.2. Phishing

Ejemplo Práctico: Ataque de Phishing por Correo Electrónico

Un atacante envía un correo electrónico que aparenta ser de una institución bancaria, solicitando al destinatario que haga clic en un enlace para "verificar su cuenta". El enlace lleva a una página falsa idéntica a la del banco, donde el usuario ingresa sus credenciales. El atacante captura estas credenciales y las utiliza para acceder a la cuenta real del usuario.

3.3. Ataques de Denegación de Servicio (DoS)

Ejemplo Práctico: Ataque de Flood SYN

Un atacante realiza un ataque de Flood SYN enviando un gran número de solicitudes de conexión a un servidor. Estas solicitudes agotan los recursos del servidor al dejar conexiones pendientes sin completarse, provocando la denegación de servicio para usuarios legítimos.

3.4. Inyección de Código

Ejemplo Práctico: Inyección de SQL

Un atacante utiliza una vulnerabilidad en un formulario web para realizar una inyección de SQL. Al introducir código SQL malicioso, el atacante puede manipular la base de datos subyacente, extraer información sensible o incluso borrar datos.

3.5. Ataques de Ingeniería Social

Ejemplo Práctico: Engaño Telefónico

Un atacante se hace pasar por un empleado del soporte técnico y llama a un usuario, alegando un problema de seguridad en su cuenta. Engañando al usuario para que revele

sus credenciales, el atacante obtiene acceso no autorizado a la cuenta de la víctima.

4. Casos prácticos

4.1. Malware

Caso Práctico: WannaCry

En mayo de 2017, el ransomware WannaCry afectó a sistemas de todo el mundo, cifrando archivos y solicitando un rescate en bitcoin para su liberación. Este ataque se propagó a través de una vulnerabilidad en el protocolo SMB de Microsoft, explotando sistemas no parcheados. Hospitales, empresas y servicios públicos fueron paralizados, demostrando la amenaza tangible que representa el malware.

4.2. Phishing

Caso Práctico: Ataque al DNC (Comité Nacional Demócrata)

En 2016, el Comité Nacional Demócrata de los Estados Unidos fue víctima de un ataque de phishing. Los empleados recibieron correos electrónicos aparentemente legítimos solicitando cambiar sus contraseñas. Al caer en la trampa, los atacantes obtuvieron acceso a correos electrónicos y documentos confidenciales, influyendo en el proceso electoral.

4.3. Ataques de Denegación de Servicio (DoS)

Caso Práctico: Ataque a GitHub en 2018

En 2018, GitHub experimentó uno de los mayores ataques DDoS registrados. El ataque, que alcanzó los 1.35 terabits por segundo, causó interrupciones temporales en el servicio. Aunque GitHub pudo mitigar el ataque rápidamente, resaltó la vulnerabilidad de plataformas clave en Internet.

4.4. Inyección de Código

Caso Práctico: Ataque a Equifax

En 2017, la agencia de informes de crédito Equifax sufrió un ataque masivo de inyección de código SQL. Los atacantes explotaron una vulnerabilidad en una aplicación web, accediendo a la base de datos y comprometiendo información personal de casi 147 millones de personas.

4.5. Ataques de Ingeniería Social

Caso Práctico: Ataque a Twitter en 2020

En julio de 2020, varias cuentas verificadas de Twitter fueron comprometidas en un ataque de ingeniería social. Los atacantes se hicieron pasar por empleados de Twitter y engañaron a otros empleados para que les otorgaran acceso a herramientas internas. Utilizando estas herramientas, publicaron mensajes fraudulentos solicitando donaciones de criptomonedas.

5. Actividades sugeridas de aprendizaje

Análisis de Malware:

Investigar el comportamiento de un malware específico y documentar cómo se propaga, las técnicas que utiliza y cómo puede ser mitigado.

Simulación de Ataque de Phishing:

Diseñar y ejecutar un simulacro de ataque de phishing en un entorno controlado, evaluando la conciencia de los usuarios y proponiendo medidas preventivas.

Mitigación de Ataques DDoS:

Configurar medidas de seguridad en un servidor web para mitigar un ataque DDoS simulado. Evaluar la eficacia de estas medidas y proponer mejoras.

Evaluación de Seguridad en Aplicaciones Web:

Realizar un análisis de seguridad en una aplicación web, identificando posibles vulnerabilidades y proponiendo soluciones para mitigar riesgos.

Pruebas de Concientización en Ingeniería Social:

Realizar pruebas de concientización en ingeniería social, simulando llamadas telefónicas o correos electrónicos falsos para evaluar la capacidad de los usuarios para identificar amenazas.

CONCLUSIONES

La diversidad y sofisticación de los ataques informáticos subrayan la importancia de la ciberseguridad en la sociedad actual. La prevención, detección y respuesta efectivas son esenciales para proteger la información y preservar la integridad de sistemas y datos.

REFERENCIAS BIBLIOGRÁFICAS

1. Chapple, M., & Schmidt, D. (2019). IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education.

2. Goodin, D. (2017, May 15). Wanna Decryptor: The ransomware worm that didn't arrive on a phishing hook. Ars Technica. [https://arstechnica.com/information-technology/2017/05/the-wannacry-ransomware-worm-that-brought-down-global-computers/]

3. Perlroth, N., & Shane, S. (2016, December 13). Russian Hackers Acted to Aid Trump in Election, U.S. Says. The New York Times. [https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html]

4. Menn, J. (2018, February 28). GitHub hit with largest-ever DDoS attack that peaked at 1.35 Tbps. Reuters. [https://www.reuters.com/article/us-github-cyber/ddos-attack-that-crippled-github-comes-back-every-wednesday-idUSKCN1GE2V6]

5. Riley, M., & Kocieniewski, D. (2017, September 20). Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop. Bloomberg. [https://www.bloomberg.com/news/articles/2017-09-20/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop]

6. Conger, K., Lee, D., & Isaac, M. (2020, July 16). Twitter Hack Appears to Stem From a 17-Year-Old's Own Goal. The New York Times. [https://www.nytimes.com/2020/07/16/technology/twitter-hack-arrest.html]