Guía de clase –Ataques informáticos

Sistemas Operativos

Docente: Mery Yolima Uribe
Desarrollo: Individual en clase
Estudiante: Luis Felipe Narvaez Gomez
Código Estudiante: 2312660

Recuerda: Documentar el proceso y subir las evidencias al campus virtual al FINALIZAR la clase

1. Seleccionar tres tipos de ataques informáticos

GUSANO
TROYANO
DENEGACION DE SERVICIOS

2. Buscar 2 ejemplos de cada tipo de ataque seleccionado

GUSANO [I love you] : escrito en el lenguaje Visual Basic Script que fue propagado mediante correo electrónico y IRC, el cual infecta la maquina que ejecuta el archivo y trata de autoenviarse mediante Outlook a toda la lista de contactos. Su procedencia es Manila Filipinas y su autor se apoda Spyder.

GUSANO [Mydoom] : es una nueva variante del anterior virus MIMAIL el cual se propaga por correo electrónico y red P2P.

> "*Este virus utiliza asuntos, textos y nombres de adjuntos variables en los correos en los que se envía, por lo que no es posible identificarlo o filtrarlo fácilmente, y utiliza como icono el de un fichero de texto plano para aparentar ser inofensivo. Tiene capacidades de puerta trasera que podrían permitir a un usuario remoto controlar el ordenador infectado, dependiendo de la configuración de la red y del sistema".*

TROYANO [Carberp]: su versión original fue un troyano clásico diseñado para robar la información confidencial de los usuarios como las credenciales bancarias o los accesos a diferentes paginas web y luego enviar estos datos a un servidor controlado por su creador.

TROYANO [Citadel]: Es una de las versiones del rey TROYANO ZEUS el cual surgió como uno de los tantos malware después de que publicara el código fuente de Zeus en el 2011.

> *"El grupo de ciberdelincuentes responsable de Citadel creó una comunidad de clientes y colaboradores a escala internacional, quienes conformaban una especie de red social criminal donde se intercambiaban ideas: cifrado AES de los archivos, la capacidad de eludir las páginas de rastreo, bloqueo del acceso a páginas de seguridad en el equipo de la víctima o eliminar los vídeos de los usuarios".*

DDOS [UDP Flood]: "*Este ataque DDoS aprovecha el protocolo UDP (User Datagram Protocol), un protocolo de red que no necesita una sesión iniciada en el equipo remoto. Este tipo de ataque*

inunda puertos aleatorios dicho host remoto con numerosos paquetes UDP , causando que el equipo víctima compruebe ante cada petición a cada puerto, si hay alguna aplicación escuchando en destino; y en caso de no haberla responde con un paquete ICMP (Internet Control Message Protocol) de error de destino. Al ser el número de paquetes enviado enormemente exagerado, este proceso agota los recursos del servidor o equipo, y en última instancia puede conducir a la inaccesibilidad".

DDOS[ICMP Flood]: *"Similar en principio al ataque de inundación UDP, este en particular satura el recurso de destino con solicitud de paquetes "eco" ICMP (más conocido como ping), básicamente se trata de enviar paquetes de solicitud sin esperar los paquetes de respuesta. Este tipo de ataque puede consumir tanto ancho de banda saliente y entrante , ya que las solicitudes intentarán ser respondidas con paquetes ICMP mientras no paran de llegar nuevos paquetes, dando como resultado una significativa desaceleración general del sistema, hasta lograr la caída del servicio o el reinicio de la máquina. Los ataques mediante ICMP flood pueden ser detenidos gracias a la configuración de Listas de Control de Acceso (ACL's) en routers y switches".*

3. Buscar casos reales o noticias sobre ataques informáticos y analizar qué lo generó, cuáles fueron los problemas presentados y cómo se solucionaron.

STUXNET, este es un malware que fue responsable de infectar los PLC´s de la central Nuclear de Natanz en Iran, por lo que es considerado como la primera ciber arma y un precedente de lo que en un futuro y presente inmediato los gobiernos deberán afrontar.
El propósito de Stunex era el de rastrear el programa nuclear iraní, la arquitectura propia en la que está funcionando físicamente la planta y atacarla. La central iraní usa centrifugas para enriquecer Uranio, centrifugas de tipo y diseño IR-1, originalmente desarrollado en Europa en los años 60 y robado por A.Q.Khan, un traficante de secretos nucleares que entrego la información a Iran en los años 80. El problema de la implementación iraní de los planos europeos, era la relativa facilidad con la que se rompían las centrifugas por su falta de robustes y es esta cualidad física la que aprovecho el Malware STUXNET para actuar.
Para evitar que las centrifugas se dañen, la presión del sistema era nivelada por válvulas controladas mediante sistemas de PLC´s la cuales liberaban la presión excedente; de la misma manera para mermar la presión sobre el sistema la velocidad formal de operación de los rotores debía mantenerse en los 63000 rpm, más de allí se obtenían fenómenos de resonancia producto de la vibración de los rotores.
STUXNET tuvo como objetivo los controladores industriales SIEMENS S7-417, encargados de controlar las válvulas y sensores de presión de las centrifugas, camuflándose como un archivo de configuración de Software de Siemens, además de que no era detectable pues para ser instalado, tuvo que ingresarse a través de USB o llevarlo a través de portátiles. El malware se encargaba de alterar medidas en lapsos de tiempo muy cortos en el periodo de operación, haciendo que poco a poco las centrifugas se dañasen o los procesos directamente se vieran comprometidos, ya sea por producción final o inherente estallido de maquinaria industrial.

WANNACRY, Este es un tipo de virus de crypto ransomware, muy utilizado por cibercriminales para extorsionar dinero atraves del encriptamiento o cifrado de archivos valiosos que quedan tener las personas o empresas blanco de los ocupantes del malware.

> *"Los orígenes de WannaCry se remontan a mayo de 2017, cuando un grupo de misteriosos piratas informáticos que se autodenominan Shadow Data Brokers lanzaron públicamente un tesoro de código NSA robado. Las herramientas incluían una técnica de piratería secreta hasta entonces conocida como EternalBlue, que explota fallos en un protocolo de Windows conocido como Server Message Block para hacerse cargo de forma remota de cualquier ordenador vulnerable.*
>
> *Varios investigadores de seguridad comenzaron a trabajar para tratar de descubrir los orígenes de WannaCry. Se indicó que el código podría tener un origen norcoreano. WannaCry había estado circulando durante meses antes de que explotara en Internet el 12 de mayo de 2017. Esta versión anterior del malware, llamada Ransom, tenía puntos en común importantes en las herramientas, técnicas e infraestructura utilizadas por los atacantes con las utilizadas por el Grupo Lazarus.*
>
> *El Grupo Lazarus es un grupo de piratería que ha sido vinculado a Corea del Norte. Comenzando su carrera en 2009 con crudos ataques DDoS en los ordenadores del gobierno de Corea del Sur, se han vuelto cada vez más sofisticados, pirateando a Sony y logrando atracos a bancos*
> *El ataque del ransomware WannaCry golpeó alrededor de 230.000 ordenadores en todo el mundo.*
>
> *Una de las primeras empresas afectadas fue la empresa española de telefonía móvil, Telefónica. Para el 12 de mayo, miles de hospitales y cirugías del NHS en todo el Reino Unido se vieron afectados.*
>
> *Un tercio de los fideicomisos del hospital del NHS se vieron afectados por el ataque. Según informes, las ambulancias fueron desviadas, lo que dejó a las personas que necesitaban atención urgente. Se estimó que le costó al NHS la friolera de 92 millones de libras después de que se cancelaron 19,000 citas como resultado del ataque.*
>
> *A medida que el ransomware se extendió más allá de Europa, los sistemas informáticos en 150 países quedaron paralizados. El ataque del ransomware WannaCry tuvo un impacto financiero sustancial en todo el mundo. Se estima que este delito cibernético causó pérdidas de 4 mil millones de dólares en todo el mundo.".*

La forma de detener el Wannacry fue mediosa, pues el parche que evitaba las infecciones ya estaba disponible antes de que comenzaran los ataques según el boletín de seguridad de Microsoft MS17-010, compañía que implemento la actualización contra el malware en su SO Windows con el protocolo SMB así evitando las infecciones por Eternal Blue. El problema sin embargo la actualización no fue instalada en muchos equipos a tiempo.