UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD DE APRENDIZAJE NÚMERO 7: ESPANOL

FECHA ENTREGA:
VIERNES 28 DE SEPTIEMBRE 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

PENTESTING

Sombrero blanco, o hacker eticos son los nombres que se le da a las personas que realizan ataques sin fines de mala fe y con enfoque de analisis a una infrestructura.
Haciendo referencia de pasadas tareas sobre :
“Bug encontrado antes de ser vulnerado entonces no es un bug”, El hacking etico podria centrarse en encontrar todas esas vulnerabilidades antes de que estan sean encontradas por un tercero y lo explote provocando perdidas en la empresa.
Si bien, es mucho mas “barato“ analisar, encontrar y parchar vulnerabilidades antes de que estas sean explotadas puesto que cuando una vulnerabilidad es explotada por un tercero esto puede conllevar perdidas millonarias.
La preparacion es la clave del exito:, L*a calidad no son salchipulpos,* se debe planear como parte de desarrollo y modelo de negocio de la empresa, desde un principio y hasta la etapa de liberacion, constante analisis y mejora continua, estar al dia con las actualizaciones de software: solo de esta manera se podra garantizar la seguridad de una infrestructura.
Pensar como el atacante: Si bien, una buena manera de prevenir un hackeo es contemplar las mismas posibilidades que podria contemplar el hacker y tomas acciones a situaciones comunes, estando **un paso adelante**: Por ejemplo, supongamos que tenemos un VPS en la internet el cual tiene multiples servicios corriendo entre ellos una Base de datos, un servidor web, un servidor ssh y un servidor de correos, estos servicios permiten el funcionamiento de un sistema de pagos de un departamento de creditos, corriendo en PHP.
Identificacion: Si bien, en primera instancia el hacker intentara identificar nuestro sistema operativo, cada uno de los servicios y los puertos abiertos en nuestro VPS; Por ello configurar el **firewall y** desactivar todos aquellos que no sean requeridos, como podria serlo el servicio de ICMP son elementales para prevenir la deteccion del Os y sus servicios.

En el caso del servicio de base de datos podriamos configurarlo para negar la conexion fuera del servidor, ya que la aplicacion esta dentro del mismo, no es requerida la conexion de cliente fuera del VPS, cambiar el nombre de administrador default, configurar correctamente los usuarios y sus permisos, contrasena segura, cambiar los puertos default. Para el servidor ssh, cambiar puertos, contrasenas y diferentes a la de otros servicios, desactivar el loggin del ususario root que existe en todo sistema linux por default. En el caso del servidor web y el servidor de correo es fundamental su correcta configuracion dado que suelen ser los mas vulnerables. De esta manera se dificulta la deteccion de servicios.

Analisis: una vez que nuestro sistema esta bien ‘tweakieado’ bien tuneado a tal grado de que solo los minimos servicios estan corriendo y pueden ser identificados, podemos proseguir a la etapa de analisis en la cual buscamos por CVE’s especificas por el servicio y version de nuestro sistema operativo y servicios, es por ello que tener actualizado nuestro sistema y servicios tienen tanto impacto, para prevenir las vulnerabilidades conocidas.

Ejecucion: Si bien, si por alguna razon en nuestro VPS’s se encuentra alguna vulnerabilidad, por ejemplo, en el servidor de correo, debemos considerar actualizar a la ultima version donde no exista dicha vulnerabilidad o incluso migrar a otro servicio con el fin de evitar la vulnerabilidad: , ya sea a traves de otro servicio u configuracion, *lo que sea necesario para que no se pueda llevar a cabo la explotacion de dicha vulnerabililidad.*

NOTICIA

https://thehackernews.com/2018/09/scan4you-malware-scanner.html
September 22, 2018

https://www.justice.gov/opa/pr/operator-counter-antivirus-service-scan4you-sentenced-14-years-prison
Friday, September 21, 2018

Un pirata informático letón detrás del desarrollo y la operación del servicio antimonopolio scan4you finalmente ha sido condenado a 14 años de prisión.

37 años de edad ruslans bondars, descrito como un letón no ciudadano o ciudadano de la antigua URSS que había estado residiendo en Riga, Letonia, fue declarado culpable el 15 de mayo en un tribunal federal en Alejandría, durante el cual un co-conspirador reveló que tenía trabajó con la aplicación de la ley rusa.

bondars creó y escaneó un total de virus como el servicio antivirus de múltiples motores en línea que permitía a los piratas informáticos ejecutar su código por varias empresas antivirus, pero en su lugar informó a sus usuarios que podían "cargar archivos anónimamente y prometió no compartir información sobre los archivos cargados". la comunidad antivitus ".

bondars fue uno de los dos hackers que ejecutó scan4you de 2009 a 2016 y ayudó a otros autores de malware a probar y mejorar el malware que "solían infligir millones de dolares en pérdidas a los consumidores y las compañías estadounidenses"

Bondars, socio de juris martisevs, quien también fue arrestado durante un viaje a Lavtia y extraditado a Estados Unidos, se

declaró culpable de cargos similares en marzo de este año.

de acuerdo con el comunicado de prensa del departamento de justicia, los clientes de Scan4you solían robar aproximadamente 40 millones de números de tarjetas de crédito y débito, y otra información personal de una tienda minorista estadounidense, causando pérdidas de $ 292 millones.

Otro cliente usó scan4you para ayudar al desarrollo de "Citadel", una mancha de malware ampliamente utilizada que infectó a más de 11 millones de computadoras en todo el mundo, incluso en los Estados Unidos, y provocó más de $ 500 millones en pérdidas relacionadas con el fraude.

"Ruslans Bondars ayudó a los desarrolladores de malware a atacar a las empresas estadounidenses". dijo el Secretario de Justicia Auxiliar Benczkoswski. "El Departamento de Justicia y sus socios encargados de hacer cumplir la ley no entienden entre proveedores de servicios como Scan4you y los hackers tehy assists: los haremos responsables de todos los daños significativos que causan y trabajaremos incansablemente para llevarlos ante la justicia, donde sea que estén. situado".

Bondars fue condenado por tres cargos, incluida la conspiración para violar la Ley de fraude y abuso informático, la conspiración para cometer fraude electrónico y la intrusión informática con la intención de causar daños y fue sentenciado a 168 meses de prisión el viernes.

Aunque el tribunal de los EE. UU. Nunca acusó a los bondars de involucrarse directamente en ninguna intrusión, los documentos judiciales muestran que utilizó malware para robar usuarios en línea y engañarlos para que compren servicios antivirus que no necesitaban.

Además, los fiscales también dicen que Scan4you era una "innovación" en malware que ha inspirado a muchos imitadores, lo que permitió que tales servicios estuvieran fácilmente disponibles en Internet.

MI OPINION

Cada vez se desarrollan mas herramientas y tecnicas informaticas y de ingenieria social para hacking y a la vez las autoridades se toman mas en serio el apego a las leyes y por ende a la busqueda y captura de cibercriminales para que paguen por sus delitos.
Si bien la gran mayoria de herramientas de hacking son mantenidas por comunidades opensources, cuales algunos de sus mismos de sus son los mismos de comunidades de hacking que se dedican a cometer delitos a empresas y gobiernos...
La moraleja de la noticia podria ser “ el que la hace la paga”
Las empresas no destinan fondos a encontrar cibercriminales, los gobiernos si!