Práctica 5

CCN-CERT. NAVEGACIÓN SEGURA CON TOR

José Ángel Dorado González

Seguridad Informática

ÍNDICE

1º)¿Qué es el CCN-CERT?

Es la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia. Surgió en el año 2006, en el seno del Centro Criptológico Nacional, y ante la necesidad de incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas sufridas por las Administraciones Públicas y los sistemas clasificados.

El CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Por lo tanto, su misión es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

El término CERT proviene de las siglas en inglés Computer Emergency Response Team y viene a definir a un equipo de personas dedicado a la implantación y gestión de medidas preventivas, reactivas y de gestión de la seguridad con el objetivo de mitigar el riesgo de ataques contra las redes y sistemas de la comunidad a la que se proporciona el servicio y ofrecer soluciones para la mitigación de cualquier incidente y sus efectos, en el menor tiempo posible.

2º)Lee el documento CCN-CERT BP/01 Principios y recomendaciones básicas en Ciberseguridad. Escribe lo que consideres una acción de ataque de nivel de peligrosidad 1, otra de nivel 2 y otra de nivel 3 (responde en cada caso con una frase breve o máximo 1-2 párrafos de máximo 30-40 palabras cada uno).

Peligrosidad 1

Este nivel sería el más frecuente y el que menor daño conlleva, sería llevado a cabo por ejemplo por un ex-empleado o por actores poco expertos, con el foco en todos los usuarios y sin ninguna preferencia.

Peligrosidad 2

Este nivel sería un punto intermedio de daño y de frecuencia, estaría provocado directamente con actores externos que tienen ánimo de lucro económico y atacarían preferentemente a instituciones financieras, compañías tecnológicas y ONGs.

Se comprende que en este nivel, las instituciones u organizaciones afectadas se verán gravemente perjudicadas, poniéndolas en un aprieto debido a que estos delincuentes seguramente solicitarán un rescate para acabar con el ataque.

Peligrosidad 3

Este nivel sería el que más daño podría realizar aunque se da con una menor frecuencia, estaría provocado principalmente por acciones patrocinadas por los estados. Las instituciones destino del ataque serían el Gobierno y AA.PP, empresas de defensa, organizaciones I+D e infraestructuras críticas.

Cabe destacar que este nivel sería el más dañino y peligroso, poniendo en jaque tanto a la sociedad como al gobierno del país afectado, debido a que se podrían caer los sistemas de información de las entidades públicas del estado.

3º)Define brevemente los conceptos (responde en una frase breve o máximo 1-2 párrafos de máximo 30-40 palabras cada uno).

- Ciberespionaje
    - Uso de las tecnologías de la información y la comunicación (TIC) por parte de personas, grupos o empresas para obtener algún beneficio económico o personal.
- Guerra híbrida
    - Teoría de la estrategia militar en el que se utilizan toda clase de medios y procedimientos ya sea la fuerza convencional o cualquier otro medio irregular como la insurgencia, el terrorismo, la migración, los recursos naturales e incluso otros más sofisticados mediante el empleo de las últimas tecnologías (guerra cibernética)
- Pirámide de daño
    - Representación gráfica que muestra una mayor o menor peligrosidad de las ciberamenazas.
- Superficie de exposición
    - Son todos los recursos que tenemos expuestos o con posibilidad de ser atacados, hoy en día se suele decir, todos los que estén conectados a internet.
- APT
    - Es una amenaza avanzada persistente que utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas.
- Ataque persistente
    - Utiliza técnicas de pirateo de forma continuada para acceder a un sistema y quedarse ahí durante un período de tiempo prolongado.
- Técnicas de exfiltración
    - Son procesos de extracción no autorizada de datos dentro de un sistema o de una red.
- Ingeniería inversa
    - La ingeniería inversa es un método de resolución. Aplicar ingeniería inversa a algo supone profundizar en el estudio de su funcionamiento, hasta el punto

de que se pueda llegar a entender, modificar y mejorar dicho modo de funcionamiento.
    - En el caso concreto del software, se conoce por ingeniería inversa a la actividad que se ocupa de descubrir cómo funciona un programa, función o característica de cuyo código fuente no se dispone, hasta el punto de poder modificar ese código o generar código propio que cumpla las mismas funciones.
- Internet profunda
    - La Internet profunda es aquella que simplemente no esta indexada por los motores de búsqueda o directorios. Es decir son páginas o mejor dicho repositorios de información, generalmente bases de datos dinámicas, cuyo contenido no puede ser revisado por los buscadores y por lo tanto incluido en sus resultados de búsqueda
- Red TOR
    - El nombre TOR son las siglas de 'The Onion Router', el router Cebolla, y es posiblemente la principal y más conocida darknet de internet. El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional.
- Bitcoins
    - Bitcoin es una moneda virtual o un medio de intercambio electrónico que sirve para adquirir productos y servicios como cualquier otra moneda.
- Cortafuegos personales
    - Es una aplicación que controla el tráfico de red hacia y desde una computadora, permitiendo o denegando las comunicaciones en función de una política de seguridad.
    - Está pensado para ser usado en un solo ordenador.
- Borrado seguro de datos
    - Es un método de borrado de archivos basado en software cuya función es sobrescribir los datos con el propósito de destruir completamente todos los datos electrónicos que residen en una unidad de disco duro u otros medios de almacenamiento.
- Navegación segura
    - Necesidad que tiene cualquier usuario (adulto o menor) de acceder a Internet con las garantías de que se respetan sus derechos.
- Cookies
    - Las cookies son pequeños fragmentos de texto que los sitios web que visitas envían al navegador. Permiten que los sitios web recuerden información sobre tu visita, lo que puede hacer que sea más fácil volver a visitar los sitios y hacer que estos te resulten más útiles.
- Ingeniería social
    - Es un conjunto de técnicas que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos y es utilizado en diversas formas de estafas y suplantación de identidad.
    - El principio que sustenta la ingeniería social es el de que, en cualquier sistema, los usuarios son el «eslabón débil».

- WPA2-AES
    - Es un protocolo cifrado de seguridad que protege el tráfico de Internet en redes inalámbricas.
    - El Estándar de Codificación Avanzada ("AES", por su sigla en inglés) es el estándar de codificación seguro autorizado por Wi-Fi.
- El término “Gobernanza” en ciberseguridad
    - Subconjunto de la gobernanza empresarial que proporciona dirección estratégica, garantiza que se alcancen los objetivos y manejo de riesgos, al mismo tiempo que supervisa el éxito o fracaso del programa de seguridad de la información de una empresa.
- Continuidad de Negocio
    - Planificación y preparación anticipada que se lleva a cabo para garantizar que una organización tenga la capacidad de seguir realizando sus funciones y actividades críticas durante eventos de emergencia o eventos disruptivos.

4º)¿Qué son los sistemas heredados (legacy) y qué problema plantean en ciberseguridad?

Es un sistema, tecnología o aplicación de software antiguo o desactualizado que sigue en uso dentro de una organización porque sigue desempeñando las funciones para las que fue diseñado. Por lo general, los sistemas legacy ya no cuentan con soporte y mantenimiento y están limitados a nivel de crecimiento.

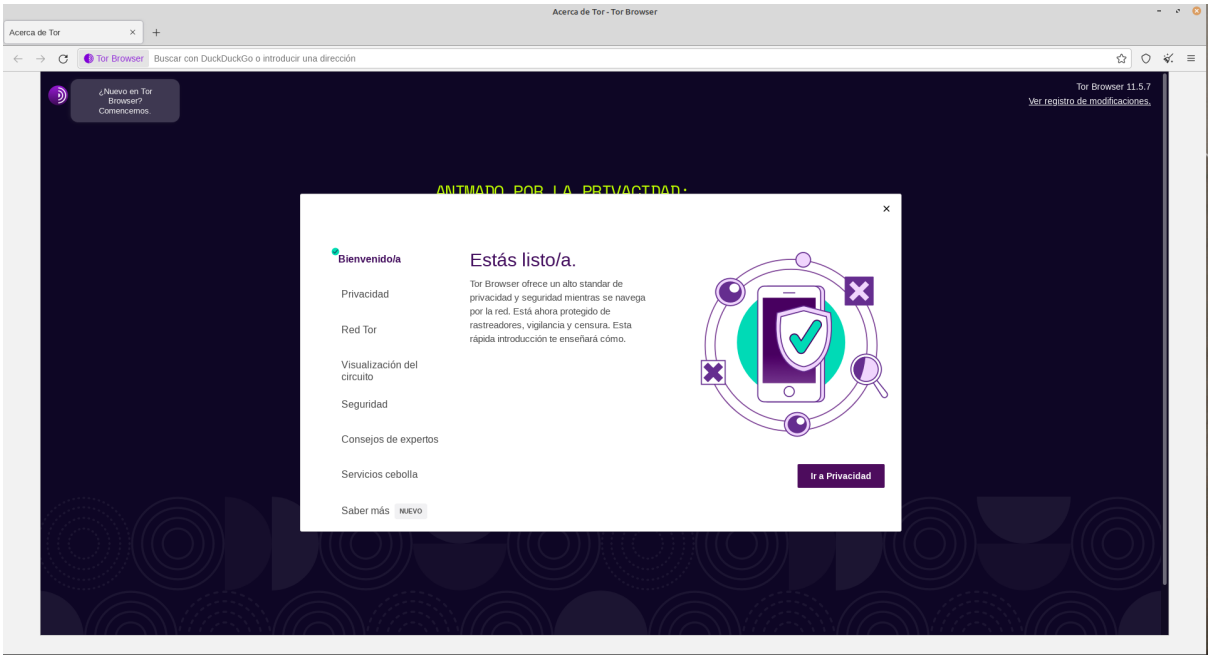
Estos tipos de sistemas que están desactualizados pueden ser un gran problema para las organizaciones que los poseen, debido principalmente a que las actualizaciones se realizan para poder corregir fallas y errores encontrados, por lo que si se encuentran anticuados tendrán mayores vulnerabilidades ante ataques maliciosos.

Estos sistemas no son fáciles de reemplazar debido a que dicho proceso es muy costoso, aunque si tenemos en cuenta que tenerlos desactualizados puede provocar que se reciba un ataque y el resultado sea mucho más difícil de solucionar, lo mejor sin duda es que sean sustituidos o actualizados.

5º)La Red TOR. Investiga online: https://www.torproject.org/es/

A. Descarga e instala en tu equipo el navegador Tor Browser. Al ejecutarlo visita la sección "¿Nuevo en Tor Browser? Conócenos!!"

Navegador Tor instalado



Sección "¿Nuevo en Tor Browser? Conócenos!!"

B. Este navegador usa como buscador por defecto DuckDuckGo, ¿Por qué crees que usa este buscador?¿Qué es DuckDuckGo? (máximo 2-3 párrafos de máximo 30-40 palabras cada uno).

DuckDuckGo es un motor de búsqueda alternativo a los grandes nombres del sector. Un motor de búsqueda son los buscadores que utilizas en sus páginas web o directamente en tu navegador si lo tienes configurado.Google es un motor de búsqueda, y DuckDuckGo es otro alternativo que no tiene tantos recursos, pero que durante los últimos años no ha parado de crecer, y ya ha superado las 1.000 millones de búsquedas mensuales.

Este buscador se utiliza debido a que su punto fuerte es que está centrado en ofrecer la mayor privacidad posible a sus usuarios. No almacena la dirección IP de sus usuarios ni guarda ninguna información relacionada con ellos, por lo que no tiene capacidad para personalizar los resultados de búsqueda. Además, tampoco comparte los datos sobre las búsquedas de los usuarios con las páginas web.

En definitiva, el navegador Tor se centra principalmente en la navegación privada, por lo que el buscador DuckDuckGo es el que mejor le conviene utilizar.

C. Describe brevemente tu experiencia con TOR y su navegador.(máximo 2-3 párrafos de máximo 30-40 palabras cada uno).

En relación a mi experiencia con TOR, podría afirmar que ha sido positiva. En primer lugar al entrar podemos ver una interfaz de usuario bastante parecida a la de otros navegadores como Google Chrome, esto facilita bastante su manejo.

He podido encontrar varios aspectos positivos que me han gustado, uno de ellos es que no se permite guardar contraseñas y usuarios como ocurre en los navegadores convencionales. Otro detalle importante es que al realizar cualquier búsqueda los resultados nos aparecen sin orden de preferencia, es decir, nos aparecen según los términos que hayamos colocado en el buscador. Todo esto permite una mayor y mejor privacidad del usuario.

Una cosa negativa que he encontrado ha sido que en algunas ocasiones las búsquedas se ralentizan y tardan más que en un buscador habitual. Esto también es producido porque TOR no está respaldado por grandes compañías como Vodafone o Telefónica.

D. Escribe uno o dos ejemplos reales y muy diferentes en los que esta red puede ser útil incluso a nivel internacional(máximo 2-3 párrafos de máximo 30-40 palabras cada uno).

Un ejemplo que se me ocurre es que lo utilicen periodistas o activistas que se encuentran en un país con una fuerte censura. Con la privacidad que ofrece TOR estas personas pueden publicar sus ideas y opiniones con el resto del mundo sin ser identificados.

Otro ejemplo podría ser para aquellas personas que se encuentran exiliadas de su país por algún motivo, con TOR se imposibilita la idea de poder rastrear la geolocalización del dispositivo de esa persona cuando accede a diferentes contenidos en la red.

En definitiva, TOR permite una privacidad absoluta al usuario por lo que será útil en todas aquellas situaciones en las que se deba ser anónimo. Sin embargo, al igual que puede ser una herramienta excelente, también puede contener sus riesgos y ser realmente peligrosa.

Bibliografía

https://www.ccn-cert.cni.es/

https://www.unodc.org/e4j/es/cybercrime/module-14/key-issues/cyberespionage.html

https://es.wikipedia.org/wiki/Guerra_h%C3%ADbrida

https://informaticapolo.com/podcast/071-superficie-de-exposicion-para-un-ataque-informatico/

https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

https://blog.segu-info.com.ar/2014/02/tacticas-de-exfiltracion-con-apt.html?m=0

https://es.wikipedia.org/wiki/Ingenier%C3%ADa_inversa

https://papelesdeinteligencia.com/internet-profunda/

https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

https://especiales.dinero.com/bitcoin/index.html

https://en.wikipedia.org/wiki/Personal_firewall

https://www.guiaspracticas.com/recuperacion-de-datos/borrado-seguro

https://www3.gobiernodecanarias.org/medusa/contenidosdigitales/FormacionTIC/cdtic2014/01ns/index.html

https://policies.google.com/technologies/cookies?hl=es

https://www.avg.com/es/signal/what-is-wpa2

https://es.linkedin.com/pulse/programa-de-gobernanza-la-seguridad-informaci%C3%B3n-qu%C3%A9-y-d-a-

https://www.lisainstitute.com/blogs/blog/que-es-continuidad-negocio-importante

https://www.stackscale.com/es/blog/sistemas-legacy/

https://www.xataka.com/basics/duckduckgo-que-principales-diferencias-google