Práctica 1

Seguridad en las redes y sistemas informáticos

Isabel Díaz Galiano 4º IDCD A

Parte 1

Buscar y analizar dos ataques importantes que hayan sido realizados durante los años 2016-2017. Se debe de indicar al menos el método de ataque utilizado, objetivos del ataque, países afectados y tiempo de actividad.

1. El Banco Central de Bangladés pierde $81 millones (febrero 2016)

SWIFT es un sistema de mensajería usado para enviar y recibir información sobre transacciones financieras, usado todos los días.

Según el New York Times, el ataque comenzó por la penetración de uno de los componentes del sistema SWIFT, el software SWIFT Alliance Access, que maneja los mensajes financieros antes de que se envíen a la interfaz SWIFT.

Para localizar el sistema SWIFT en la red del sistema bancario, los atacantes ejecutaron primero un ataque de tipo APT que duró un año e incluyó varios malwares. Habiendo comprometido un host, los atacantes se movieron host a host, explorando la red.

Cuando el sistema SWIFT fue finalmente localizado, los atacantes monitorearon el funcionamiento de los mensajes SWIFT, por lo que pudieron enviar con éxito mensajes SWIFT fraudulentos. Vieron que el protocolo bancario incluía mostrar los mensajes SWIFT para su revisión, por lo que el malware fue diseñado para ocultar los mensajes fraudulentos de los logs y eliminarlos de las listas de transferencias. Pero un error en el deletreo de una palabra, “Fundation”, disparó las alarmas sobre un posible ataque.

Método de ataque	*Objetivos del ataque*	*Países afectados*	*Tiempo de actividad*
Malware	Robo de dinero	Bangladés Filipinas Estados Unidos	1 año

Referencias:
https://www.incibe.es/sala-prensa/notas-prensa/incibe-publica-el-ranking-los-10-principales-incidentes-ciberseguridad
https://blog.securityscorecard.com/2016/04/01/bank-heist-central-bank-bangladesh/
http://cdn2.hubspot.net/hubfs/725085/Fact_Sheets/2016-09-ILL-1376--w-Attackerbrief-BangladeshSWIFT.pdf

2. WannaCry (mayo 2017)

El 12 de mayo de 2017 una nueva versión de ransomware afectó a ordenadores de todo el mundo, incluyendo instituciones públicas y grandes organizaciones. Es un tipo de ransomware capaz de extenderse a través de toda la red de una organización explotando vulnerabilidades críticas en sistemas Windows, que ya había parcheado Microsoft en Marzo de 2017 (`MS17-010`). El exploit, conocido como “Eternal Blue”, fue filtrado en Internet por un grupo conocido como “Shadow Brokers”, en abril de 2017.

WannaCry busca y cifra diferentes tipos de archivos y añade `.WCRY` al final del nombre del archivo. Pide a los usuarios pagar $300 en bitcoins. La nota que aparece en la pantalla del ordenador avisa de que la cantidad a pagar será doblada después de tres días. Si no se ha pagado después de siete días, los archivos cifrados serán eliminados.

```
.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .ott, .sxw, .stw, .uot,
.3ds, .max, .3dm, .ods, .ots, .sxc, .stc, .dif, .slk, .wb2, .odp, .otp,
.sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3,
.sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf,
.ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .ps1, .vbs, .dip, .dch,
.sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf,
.fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .3gp, .mkv, .3g2,
.flv, .wma, .mid, .m3u, .m4u, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm,
.raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar,
.tgz, .tar, .bak, .tbk, .bz2, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi,
.sldm, .sldx, .sti, .sxi, .602, .hwp, .snt, .onetoc2, .dwg, .pdf, .wk1,
.wks, .123, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst,
.potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm,
.xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm,
.dot, .docm, .docb, .docx, .doc
```

Método de ataque	*Objetivos del ataque*	*Países afectados*	*Tiempo de actividad*
Ransomware	Cobrar por rescate económico	Rusia Ucrania India Taiwán Gran Bretaña España Alemania	1 día

Referencias:
https://www.wired.com/story/2017-biggest-hacks-so-far/
https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

Buscar información sobre las acciones y programas de espionaje de la NSA. Analizar las técnicas, procedimientos y colaboraciones realizadas.

PRISM
PRISM es el nombre de un programa de espionaje de la NSA (United States National Security Agence), quien a través de él colecciona información electrónica privada perteneciente a usuarios de servicios grandes de Internet como Gmail, Facebook, Outlook y otros. La idea básica es que permite a la NSA solicitar datos sobre personas específicas de compañías como estas. El gobierno de Estados Unidos insiste en que sólo tiene permitido coleccionar datos cuando tiene permiso del Tribunal de Vigilancia Extranjera de Estados Unidos (Foreing Intelligence Surveillance Court), un tribunal estadounidense creado y autorizado por la Ley de Vigilancia de la Inteligencia Extranejera (Foreign Intelligence Surveillance Act, FISA) en 1978.

Edward Snowden, de 29 años, trabajador de la NSA, la CIA y Booz Allen Hamilton, confesó la responsabilidad de la filtración de los documentos PRISM. Se develó tres días después de las publicaciones de los documentos. En una entrevista declaró que estaba motivado por el deber civil a filtrar información clasificada. Dejó los Estados Unidos antes del filtrado para evitar ser capturado, refugiándose en Hong Kong. Con la ayuda de WikiLeaks, se movió a Moscú y ha solicitado asilo en Ecuador, Rusia y otros países.

PRISM recoge tanto metadatos como contenidos. Un analista empieza introduciendo “selectores” (términos de búsqueda) en un sistema como PRISM, que entonces busca la información de otros programas de colección de datos o SIGADs. Los SIGADs reciben tareas de colección de diferentes tipos de datos, por ejemplo, uno llamado NUCLEON recoge los contenidos de conversaciones telefónicas, mientras que otros como MARINA almacenan metadatos de Internet.

Referencia:
https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

XKEYSCORE

Este programa permite a los analistas con acceso a los datos buscar entre gigantescas bases de datos de correos electrónicas, chats o historiales de navegación de millones de personas. Xkeyscore cuenta con servidores por todo el mundo, en países como Estados Unidos, México, Brasil, Reino Unido, España, Rusia, Nigeria, Somalia, Pakistán, Japón, Australia y Nueva Zelanda, entre otros.

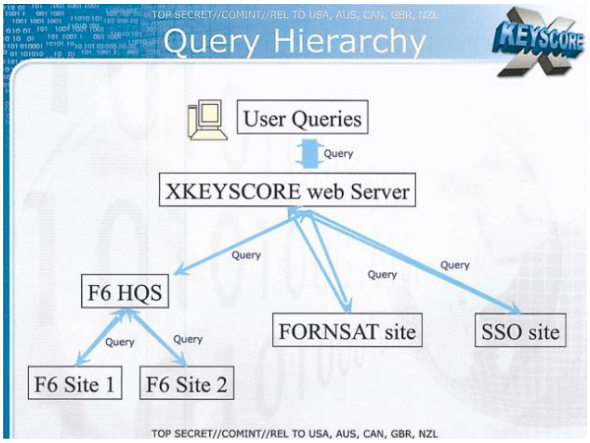
Es un sistema complejo y hay diferentes interpretaciones sobre sus capacidades reales. Para Edward Snowden, por ejemplo, es un sistema que permite casi espionaje ilimitado de cualquier persona en el mundo, mientras que la NSA ha dicho que el uso del sistema es limitado y restringido.

Xkeyscore recibe información de de estos sistemas:

- F6 (Special Collection Service): operación colectiva de la NSA y la CIA que lleva a cabo operaciones clandestinas incluyendo espionaje de diplomáticos y líderes extranjeros.

- FORNSAT (Foreign Satellite Collection): intercepciones mediante satélites.

- SSO (Special Source Operations): división de la NSA que coopera con proveedores de telecomunicaciones.



Aún así, el sistema obtiene continuamente tal cantidad de datos de Internet que esta sólo puede ser almacenada por cortos períodos de tiempo. El contenido de los datos se almacena por sólo tres o cuatro días, mientras que los metadatos se almacenan hasta treinta días.

Referencias:
https://en.wikipedia.org/wiki/XKeyscore
https://www.fayerwayer.com/2015/07/como-funciona-xkeyscore-el-buscador-de-la-agencia-nacional-de-inteligencia-nsa/
https://actualidad.rt.com/actualidad/179117-programa-espia-xkeyscore-nsa

TEMPORA

Tempora es el nombre de un sistema usado por el GCHQ (Government Commnications Headquarters). Este sistema es usado para capturar la mayoría de las comunicaciones en Internet que son extraídas de cables de fibra óptica, de forma que estas pueden ser procesadas más tarde. Fue probada desde 2008 y se convirtió en operacional en otoño de 2011.

Tempora usa interceptores en los cables de fibra óptica que componen el backbone de Internet para obtener acceso a grandes cantidades de datos personales de usuarios, sin ningún objetivo individual. Los interceptores están situados en Reino Unido, con el conocimiento de las compañías dueñas de los cables.

La existencia de Tempora fue revelada por Edward Snowden en mayo de 2013. Los documentos que adquirió declaraban que los datos coleccionados por el programa Tempora son compartidos con la NSA.

Los analistas examinan los datos recogidos. Usan una técnica llamada Massive Volume Reduction (MVR). Las descargas P2P, por ejemplo, son clasificadas como “tráfico de alto volumen, bajo volumen” y descartadas por un filtro inicial. Esto reduce el volumen de información en un treinta por ciento. Usan búsquedas específicas, que pueden referirse a palabras clave, emails de interés, o personas objetivo y números de teléfono.

Referencias:
https://en.wikipedia.org/wiki/Tempora
http://www.wired.co.uk/article/gchq-tempora-101

QUANTUM Y FOXACID

El primer paso de este proceso es encontrar usuarios de Tor. Para conseguir esto, la NSA se apoya en su gran capacidad de monitorear grandes partes de Internet. La NSA crea fingerprints que detectan solicitudes HTTP desde la red Tor a servidores particulares. Estas fingerprints se cargan en sistemas de bases de datos como Xkeyscore. Usando herramientas de análisis de datos como TURBULENCE, TURMOIL y TUMULT, la NSA busca conexiones Tor por la gran cantidad de tráfico de Internet que ve.

Una vez que se ha identificado un usuario de Tor individual, la NSA usa su red de servidores secretos de Internet para redirigir a esos usuarios a otro conjunto de servidores secretos de Internet, llamado FoxAcid, para infectar el ordenador del usuario. Con la ayuda del sistema intermediario FoxAcid la NSA puede lanzar ataques preparados contra los ordenadores objetivo.

Una vez que el ordenador es atacado con éxito, secretamente llama a un servidor FoxAcid, que lleva a cabo ataques adicionales en el ordenador objetivo para asegurar que resulta comprometido un tiempo largo y continúa proporcionando información a la NSA.

Tor es una herramienta de anonimato bien diseñada y robusta, y atacarla con éxito es difícil. La NSA aprovecha vulnerabilidades de los navegadores Firefox de los usuarios de Tor, y no de la aplicación Tor directamente. Esto también es difícil. Los usuarios de Tor frecuentemente desactivan servicios vulnerables como scripts y Flash cuando usan Tor, haciendo difícil dirigirse a esos

servicios. Aun así, la NSA usa una serie de vulnerabilidades nativas de Firefox para atacar a usuarios del navegador Tor.

Para que los objetivos caigan en visitar un servidor FoxAcid, la NSA se apoya en sus asociaciones con compañías de telecomunicaciones estadounidenses. Como parte del sistema TURMOIL, la NSA coloca servidores secretos, llamados Quantum, en sitios clave del bakcbone de Internet. Esta localización asegura que ellos pueden reaccionar más rápido de lo que pueden otros sitios web. Explotando la diferencia de velocidad, estos servidores pueden suplantar un sitio web visitado antes de que el sitio web legítimo pueda responder, haciendo que el navegador del objetivo visite un servidor FoxAcid.

Es un ataque “man-in-the-middle”.

Los servidores FoxAcid son públicos en Internet, Tienen nombres de dominio con una apariencia normal, y pueden ser visitados por cualquier navegador desde cualquier sitio.

Sin embargo, si un navegador trata de visitar un servidor FoxAcid con una URL especial, llamada etiqueta FoxAcid, el servidor intenta infectar ese navegador, y entonces el ordenador, en un esfuerzo por tomar control de él.

El material de entrenamiento de la NSA declara que intentar visitar la página inicial de un servidor FoxAcid real no resultará en ningún ataque, y que una URL especializada es requerida. Esta URL sería creada por TAO para una operación de la NSA específica, y única a esa operación y objetivo, Esto permite al servidor FoxAcid saber exactamente quién es el objetivo y cuándo su ordenador contacta con él.

Referencia:
https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

BULLRUN Y EDGEHILL

BULLRUN es un programa de la NSA dirigido a descifrar tráfico de red cifrado. Las capacidades de descifrado incluyen insertar vulnerabilidades en herramientas comerciales de cifrado y sistemas IT, en colaboración con otras agencias de inteligencia y "técnicas matemáticas avanzadas". El programa tiene la habilidad de descifrar datos transportados a través de grandes proveedores de comunicaciones y herramientas P2P como Skype.

Se cree que la NSA ha insertado puertas traseras criptográficas en un estándar publicado por el National Institute of Standards and Tecnology (NIST) y la International Organization for Standardization (ISO), y de haber pagado a una compañía de software estadounidense para implementar el imperfecto estándar.

GCHQ tiene un programa similar llamado EDGEHILL. GCHQ ha estado trabajando en desarrollar métodos para descifrar el tráfico de Hotmail, Google, Yahoo y Facebook, y propuso un sistema para descifrar datos desde los sistemas de "pinchado" de los cables de fibra óptica como TEMPORA en "casi tiempo real".

Referencias:
http://www.dcssproject.net/bullrun/
https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

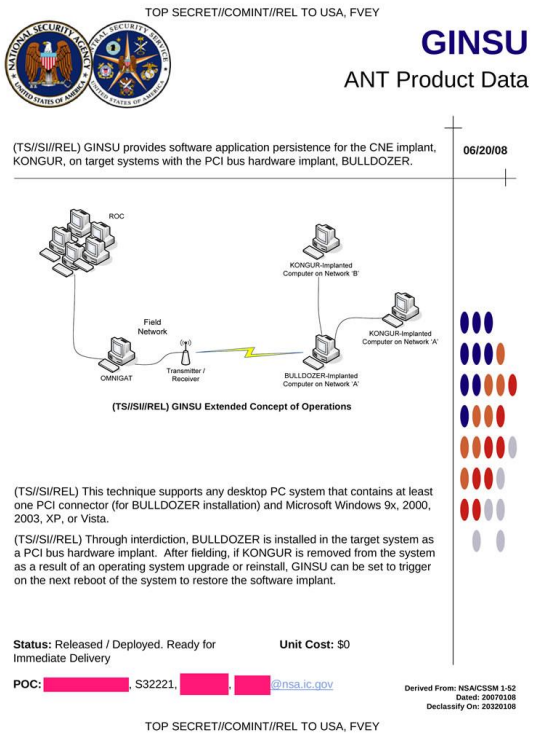
Referencias generales:
https://en.wikipedia.org/wiki/Five_Eyes
http://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden_0_240426730.html

Analizar posteriormente dos proyectos a elección del alumno que se encuentren dentro del catálogo ANT TAO de la NSA, destacando los detalles de los mismos.

El TAO y la ANT son dos divisiones de la NSA especializadas en espiar a los objetivos más difíciles. En concreto TAO son las siglas de Tailored Access Operations, Oficina de Operaciones de Acceso Adaptado. Se trata de una unidad especial de espionaje de la NSA, que se ocupa de espiar a los objetivos que la agencia no es capaz de monitorear mediante sus otros programas. La principal manera es la instalación de software y hardware espía, que bien incrustan en las máquinas de manera remota a través de Internet o bien de forma física interceptando los equipos informáticos.

La pregunta es de dónde salen las piezas de software y hardware espía. Aquí es donde entra en juego el grupo ANT, la otra "unidad élite" de la NSA que trabaja mano a mano con los de TAO y quienes según los informes a los que tuvo acceso el rotativo Der Spiegel desarrollaron diversas herramientas que les permiten crear puertas traseras en los dispositivos y programas de los grandes de la tecnología (Cisco, Dell, Western Digital…).

Estas herramientas son las que aparecen en un documento de 50 páginas con formato de catálogo de productos. De este catálogo los empleados de la NSA pueden pedir tecnologías de la división ANT para "pinchar" los datos de sus objetivos.


TOP SECRET//COMINT//REL TO USA, FVEY

GINSU

ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

06/20/08

ROC

KONGUR-Implanted Computer on Network 'B'

Field Network

KONGUR-Implanted Computer on Network 'A'

OMNIGAT

Transmitter / Receiver

BULLDOZER-Implanted Computer on Network 'A'

(TS//SI//REL) GINSU Extended Concept of Operations

(TS//SI//REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

GINSU

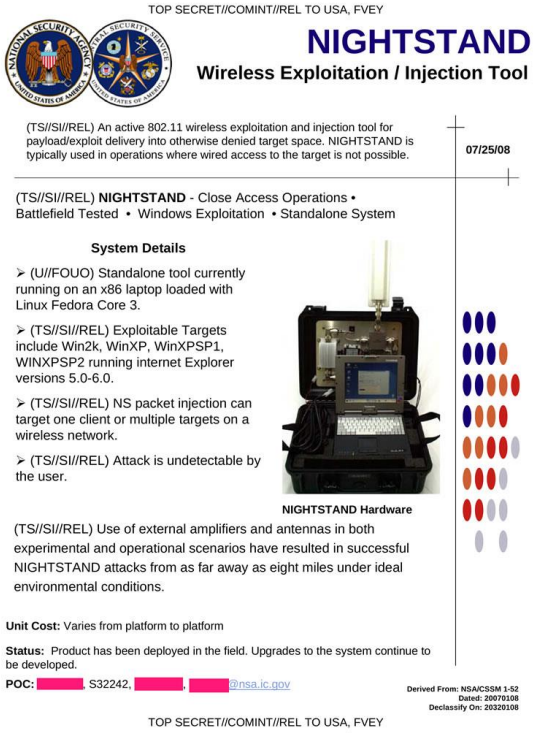
Las puertas traseras hardware y firmware requieren tener en las manos el sistema objetivo real, esto es, el objeto físico. En algunos casos, los operadores de la NSA instalan puertas traseras en el hardware y el firmware directamente en los sistemas en lo que laman “interdicción”, los sistemas son desviados durante su reparto a “estaciones de carga” donde los componentes de espionaje son instalados (esta intercepción a lo mejor ha sido conseguida con la cooperación de compañías de reparto u otras agencias gubernamentales; los detalles no están claros). En otros casos, la NSA usa un USB o herramientas de acceso remoto para obtener acceso a los sistemas, permitiendo a la NSA “reflashear” sus firmware BIOS de bajo nivel.

De una u otra forma, estas puertas traseras pueden sobrevivir al formateo de un sistema operativo. (ver SWAP attack).

Para los sistemas en los que un ataque a la Bios es irrealizable, la NSA tiene otras herramientas para instalar una puerta trasera **persistente**. Una, llamada GINSU, usa un dispositivo bus PCI instalado en el ordenador. Un implante llamado BULLDOZER crea un puente wireless sigiloso, proporcionando un control remoto basado en radio de la puerta trasera a los operadores TAO. Si el rootkit en el sistema, llamado KONGUR, es eliminado por una reinstalación del sistema, la puerta trasera GINSU puede reinstalar el software en el siguiente encendido.

NIGTHSAND

Para redes a las que la NSA no puede acceder físicamente, está NIGHTSAND, un sistema de hacking Wi-fi autocontenido que puede entrar en redes hasta 8 millas alejadas, en condiciones óptimas. NIGHTSAND hace un hijack a la red objetivo y usa ataques de inyección de paquetes para instalar exploits en los ordenadores de la red objetivo. Combinado con un exploit de Windows llamado SOMBERKNAVE, que usa un adaptador Wi-Fi del ordenador para enviar datos, puede ser usado para recoger datos de los ordenadores objetivo incluso si no están intencionadamente conectados a una red.


TOP SECRET//COMINT//REL TO USA, FVEY

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

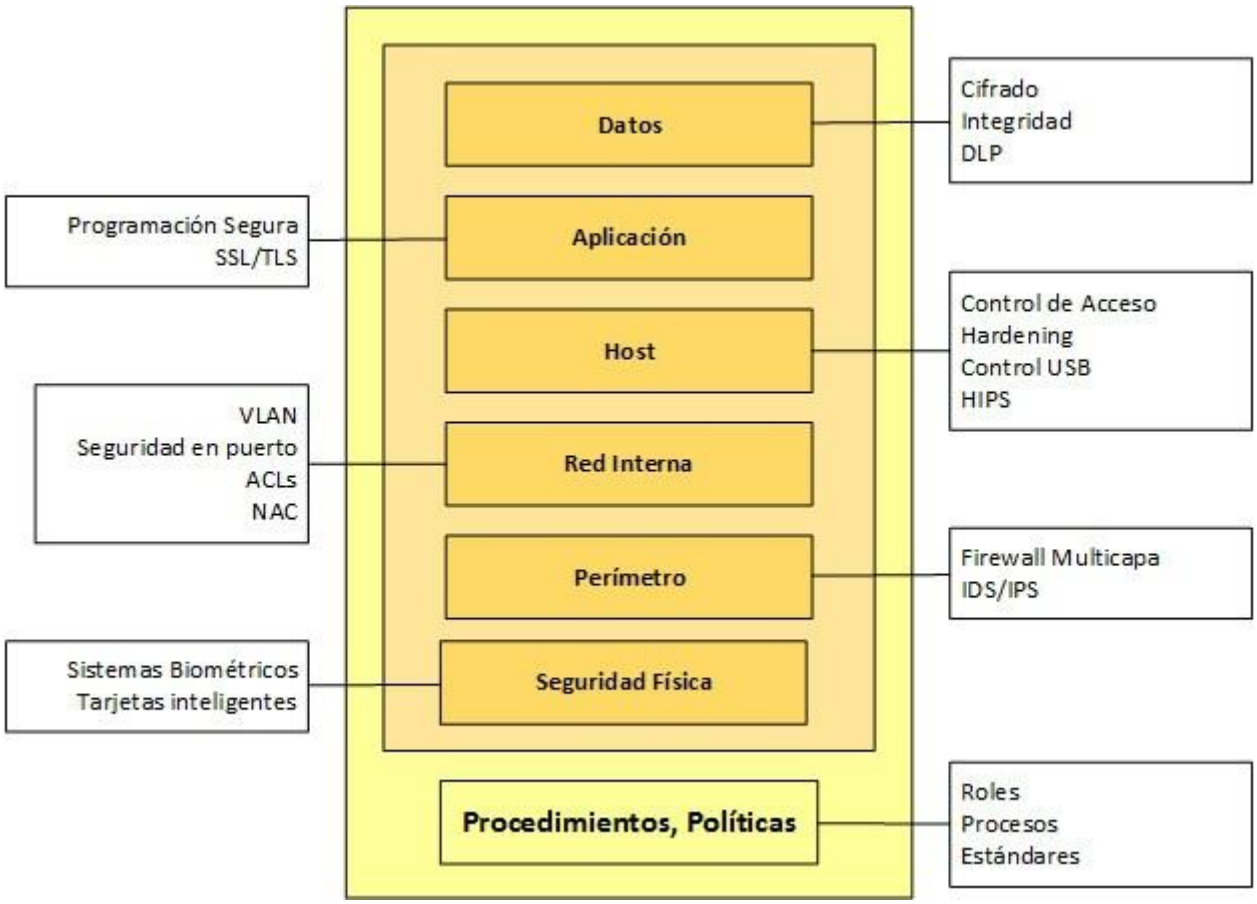
POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Referencias:
http://www.ticbeat.com/tecnologias/tao-ant-las-fuerzas-especiales-de-espionaje-de-eeuu/
http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html
https://en.wikipedia.org/wiki/NSA_ANT_catalog
https://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/

Buscar información e identificar como se implanta el modelo de defensa en profundidad en las organizaciones actualmente.



La defensa en profundidad fue desarrollada para defender un grupo militar o estratégico creando capas de defensa que forzaran al atacante a gastar una gran cantidad de recursos, mientras que se preparaban los refuerzos. El objetivo táctico es retrasar y hacer el ataque del enemigo insostenible. El defensor puede entonces contraatacar al enemigo y eliminar la amenaza.

La defensa en profundidad, en su concepto original, funciona para una defensa del mundo físico. El problema en la ciber defensa es que es insostenible. Además, si se practica en un sector civil, no se va a contraatacar para destruir al enemigo.

La defensa en profundidad consiste en implementar distintos controles y barreras con el fin de frenar la actividad de un usuario o software malicioso. De esta manera, la explotación de una vulnerabilidad o debilidad no compromete a toda la organización.

El primer paso es disponer de un inventario exhaustivo y actualizado de los equipos, tecnologías y aplicativos. Luego definiremos la importancia y criticidad que tienen para nuestra empresa y llevaremos a cabo una evaluación de riesgos que nos permita establecer un plan de diseño para asegurarlos. Finalmente, en función de esto último, consideraremos las mejores medidas tanto humanas como técnicas para alcanzarlo.

- **Procedimientos y Políticas de seguridad propias de la organización**: estándares establecidos y roles que ocupa cada responsable dentro de la empresa.

- **Seguridad física**: requiere algún tipo de identificación. También pueden ser cámaras de vídeo o personal de seguridad.

- **Seguridad perimetral**: Firewalls. Además de considerar IPs y puertos de origen y destino, tenemos NGFWs (Next Generation Firewall) que disponen de filtrado a nivel de aplicación, Deep Packet Inspection, motores antivirus, IDS/IPS, Sanboxes, VPN. NIDS (Network Intrusion Detection System) es otro de los dispositivos que nos podemos encontrar.

- **Red interna**: separar el tráfico mediante VLANs, ACLs de tal manera que sean los propios equipos de red los que permitan o denieguen cierto tipo de comunicaciones antes de llegar a los firewalls, seguridad en puerto y un NAC (Network Access Control).

- **Host**: Directorio Activo, bastionado del sistema, limitar el uso de dispositivos ISB, HIDS, esto es, funcionalidades IDS/IPS a nivel de host para detectar cualquier intento de intrusión, antivirus.

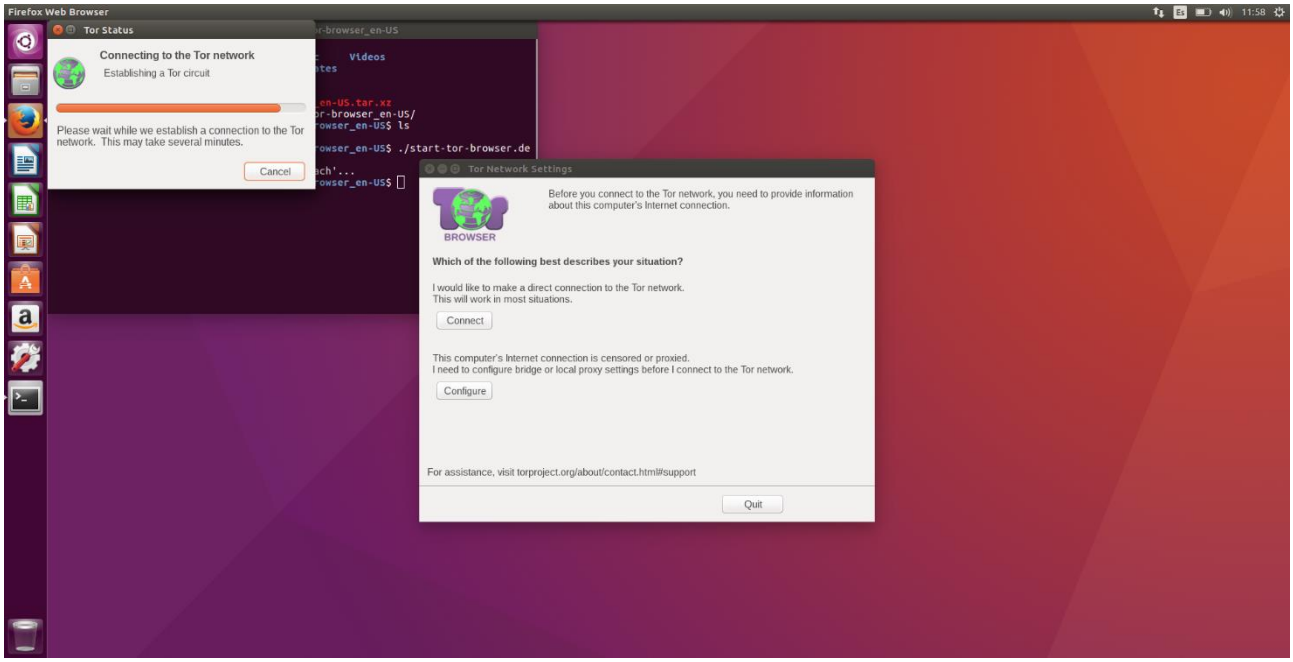
- **Aplicación**: programación segura de las aplicaciones y evitar así errores en el código que permitan a un explioit aprovechar vulnerabilidades y llevar a cabo distintos tipos de ataques, uso de protocolos para el cifrado de las comunicaciones, configuración de las redes, evitando las configuraciones por defecto, y que se ejecuten sólo con aquellos permisos y recursos necesarios para su operativa.

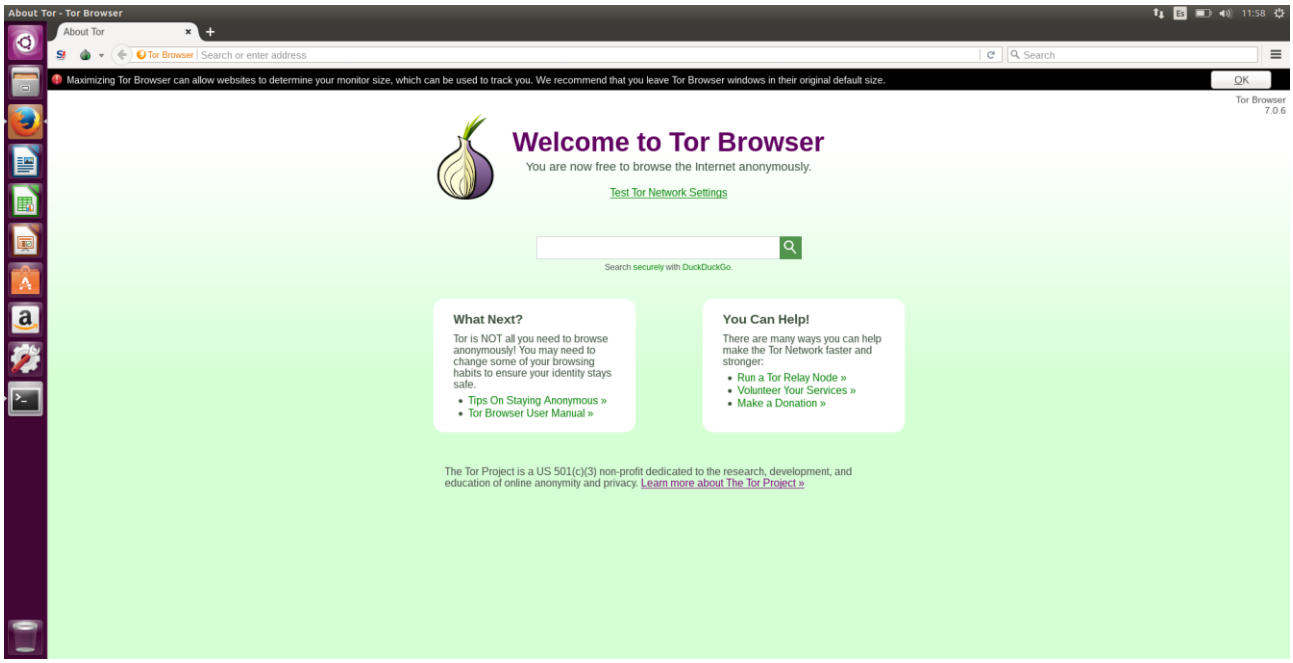
- **Datos**: Garantizar su integridad, confidencialidad y autenticación es primordial. Data Loss Prevention con el fin de que los datos puedan ser extraídos de los sistemas que los albergan con el fin de perder el control sobre los mismos, uso de algoritmos robustos.

Referencias:
https://seguinfo.wordpress.com/2008/12/03/defensa-en-profundidad-defense-in-depth/
https://enredandoconredes.com/2015/10/20/defensa-en-profundidad-breve-repaso/
https://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896

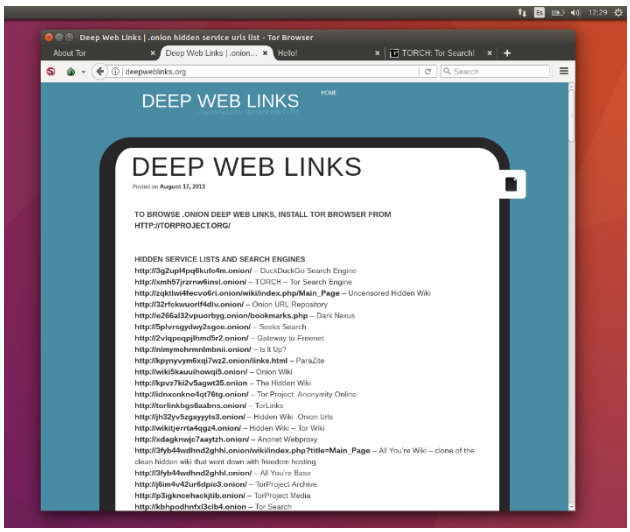
Instalar y hacer uso de TOR para acceder a la 'Deep Web'. Investigar la existencia de buscadores web TOR y utilizarlos para buscar información.

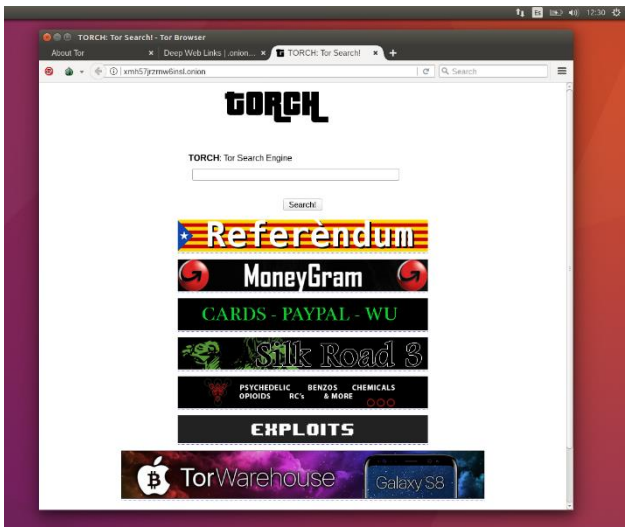
- Descargar el paquete Tor Browser y ejecutar el comando `./start…` (ver la siguiente imagen).



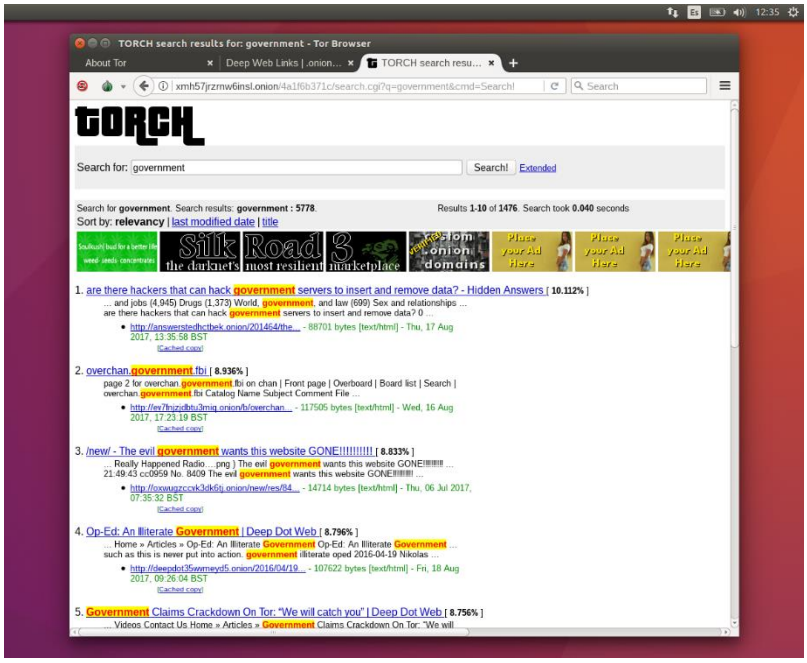


Tras deshabilitar todos los scripts en el navegador, buscar enlaces `.onion` en el buscador. Para ello, entrar en http://deepweblinks.org/.

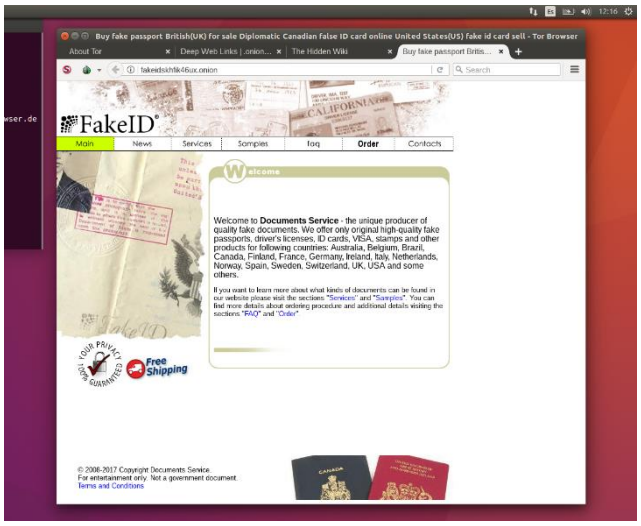


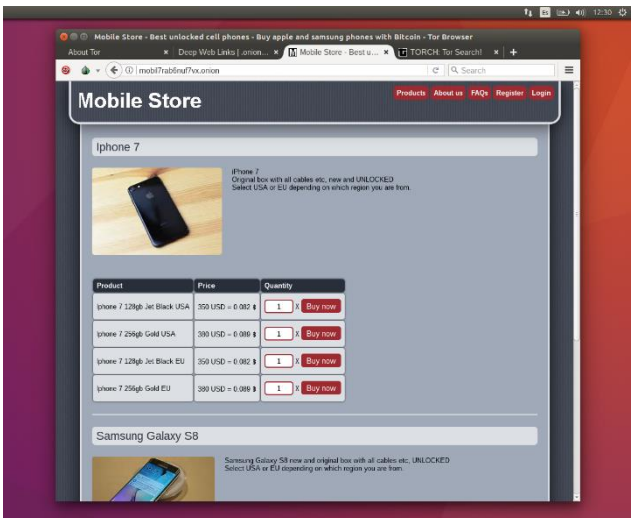


Realizar alguna búsqueda en Tor:



Algunas páginas más:





Identificar los diferentes tipos de denegaciones de servicio existentes.

Un ataque DoS consiste en inundar de tráfico un sistema o una red hasta que no sea capaz de dar servicio a usuarios legítimos. Al crear tanto tráfico pueden pasar dos cosas: que las máquinas responsables de responder a las peticiones no den más de sí o que el ancho de banda de la red no pueda procesar tantos datos. Al no poder seguir prestando un servicio, se dice que éste ha sido denegado. Además, un DoS puede ser distribuido (DdoS), lo cual es más difícil de gestionar que uno centralizado porque el tráfico se genera desde varios puntos.

Técnicas

- **Inundación ICMP**: el objetivo es inundar el ancho de banda de la víctima del ataque mediante el envío de un gran número de paquetes ICMP Echo Request (ping), y, ya que la víctima tiene que responder a esos paquetes con ICMP Echo Reply, llegará un momento en el que el volumen será tan grande que tanto el ancho de banda como la capacidad de proceso del servidor se verán comprometidos, llegando al punto de que el objetivo no puede responder a otras peticiones.

- **Ataque Smurf**: es una variante del ataque anterior. Consiste en enviar paquetes ICMP Echo Request (ping) a un intermediario con una IP de broadcast usando como dirección origen la dirección de la víctima. Por cada ICMP Echo Request que enviemos simulando ser la víctima (spoofing), la víctima recibiŕa tantos paquetes ICMP Echo Reply, es decir, una inundación ICMP multiplicada por el total de equipos en la red.

- **Inundación SYN**: Cuando se inicia una conexión TCP entre un cliente y el servidor, se ejecuta el llamado saludo a tres bandas, durante el cual normalmente el cliente envía un mensaje SYN (synchronize) al servidor, este le responde con un mensaje SYN-ACK (synchronize aknowledge) y finalmente el cliente envía un ACK (aknowledge) con lo que la conexión queda establecida.

  Durante este proceso de saludo a tres bandas, el servidor espera durante un tiempo determinado a recibir el ACK final por parte del cliente, ya que por ejemplo una congestión de tráfico puede hacer que este ACK no llegue al instante. El ataque de inundación de SYN consiste en que el atacante envía una gran cantidad de SYN, sin llegar a completar el saludo a tres bandas con el ACK final, con lo que el servidor permanece con un gran número de peticiones a medio completar con lo que no es capaz de atender las peticiones legítimas.

Referencias:
https://geekytheory.com/que-es-un-ataque-de-denegacion-de-servicio-dos
https://cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii
https://www.xatakamovil.com/conectividad/que-es-un-ddos-o-un-ataque-distribuido-de-denegacion-de-servicio

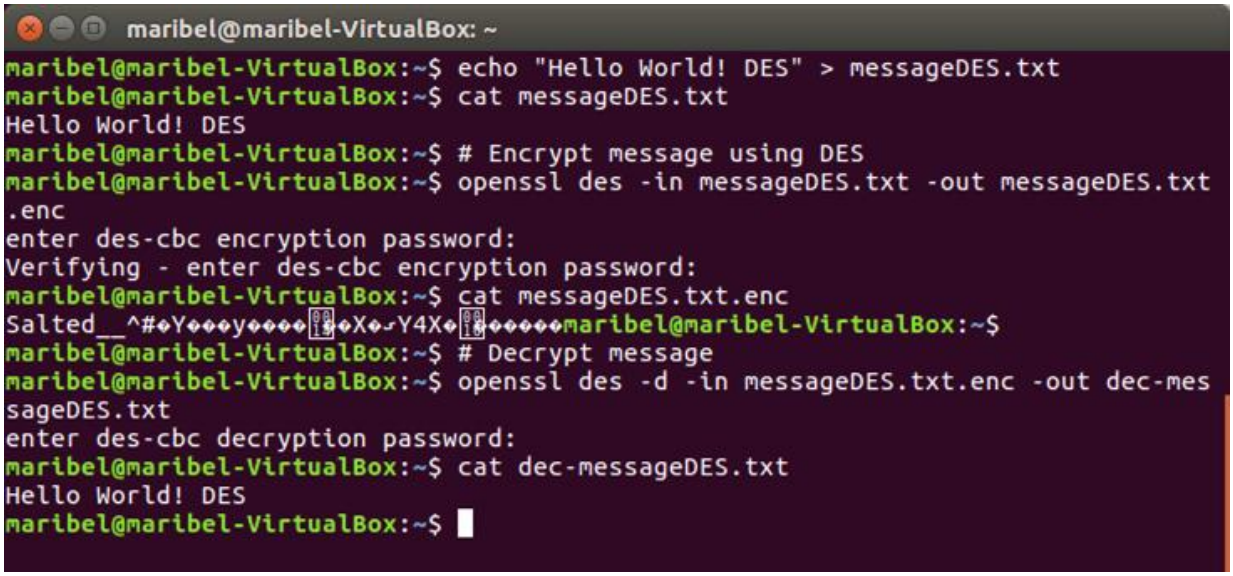
Parte 2

- **Cifrado simétrico**:

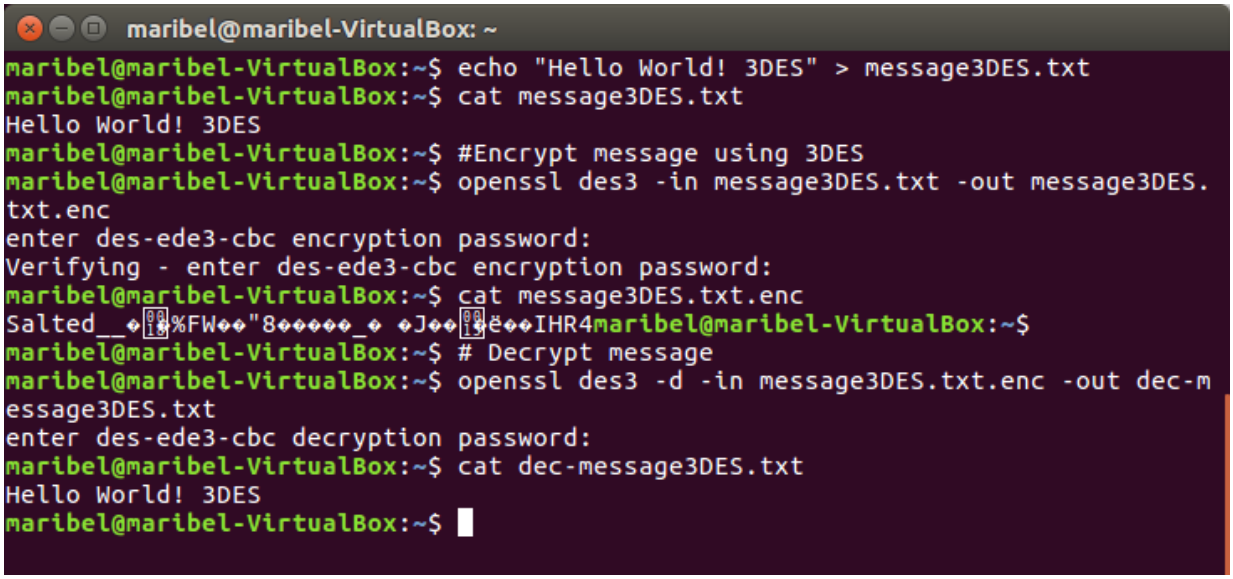
  Utilizar OpenSSL para cifrar un determinado texto mediante DES, 3DES y AES. Describir el proceso, comandos y mostrar pantallazos.

  Que es, para que sirve y cómo se puede utilizar en el cifrado simétrico. Resumir en menos de una hoja.

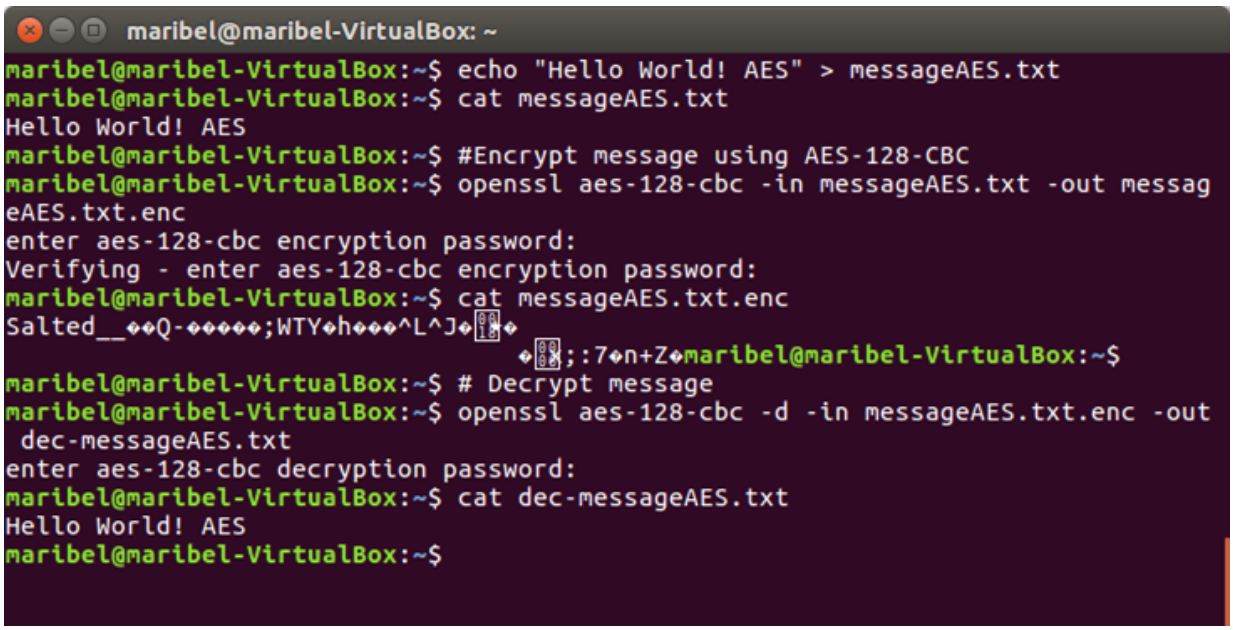
  Algoritmo DES:



  Algoritmo 3DES:



  Algoritmo AES:



Las lookup tables y las rainbow tables sólo funcionan porque cada contraseña es hasehada de la misma manera. Si dos usuarios tienen la misma contraseña, tendrán los mismos hashes. Una manera de prevenir esto es aleatorizando los hashes, de manera que dos contraseñas iguales ya no tendrán los mismos hashes.

Esto se puede hacer añadiendo como sufijo o prefijo un string aleatorio, llamado salt, a la contraseña antes de hashearla. Por eso, añadiendo diferentes salts, obtienes diferentes hashes.

El salt no tiene por qué ser secreto. Un atacante no podrá saber por adelantado que salt vas a utilizar, por lo que no van a poder pre-computar, por ejemplo, una lookup table o una rainbow table.

El salt debería ser generado usando un Cryptographically Secure Pseudo-Random Number Generator (CSPRNG). Los CSPRNGs son muy diferentes de los generadores de números pseudo-aleatorios ordinarios, como la función `rand()` del lenguaje C. Los CSPRGs proveen un alto nivel de aleatoriedad y son completamente impredecibles.

Referencias:
https://en.wikipedia.org/wiki/Salt_(cryptography)
https://crackstation.net/hashing-security.htm
https://crypto.stackexchange.com/questions/1776/can-you-help-me-understand-what-a-cryptographic-salt-is

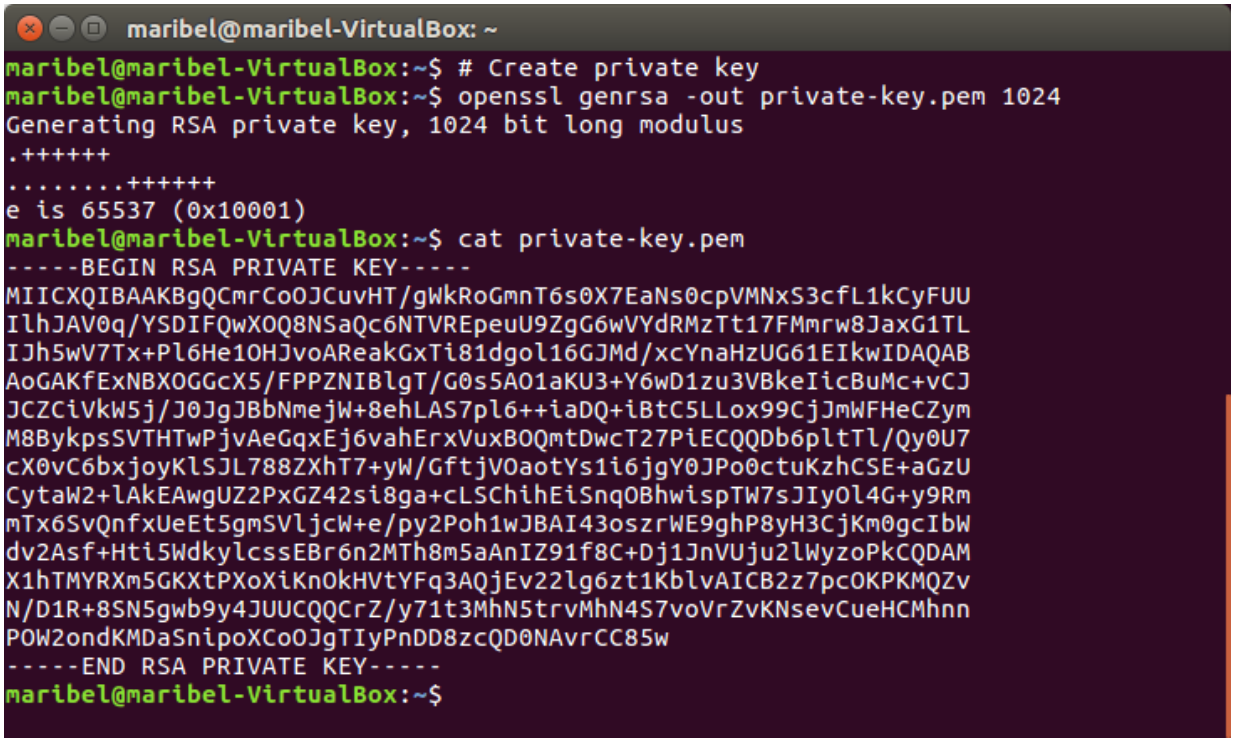
- **Cifrado asimétrico:**

  Describir el proceso, comandos y mostrar pantallazos.

  Generación de claves privada y pública. Cifrado de información con las claves generadas.

Uso de cifrado asimétrico para la conexión por SSH.

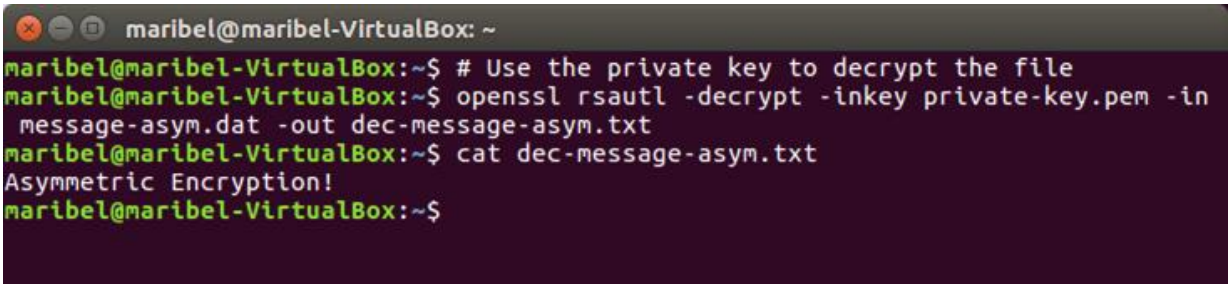
Generación de una clave privada:



Generación la clave pública a partir de la privada que acabamos de generar:

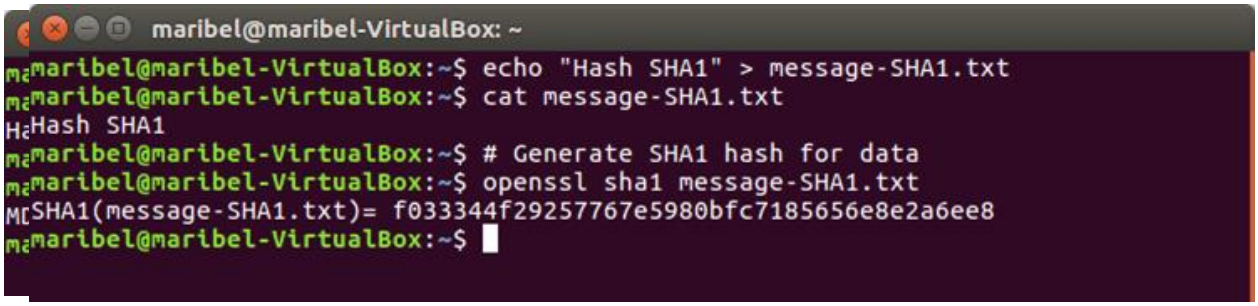
Uso de la clave pública para cifrar los datos:

Uso de la clave privada para descifrar los datos:



- **Funciones hash**:

  Utilizar OpenSSL para obtener el hash de una determinada cadena en MD5 y SHA1.



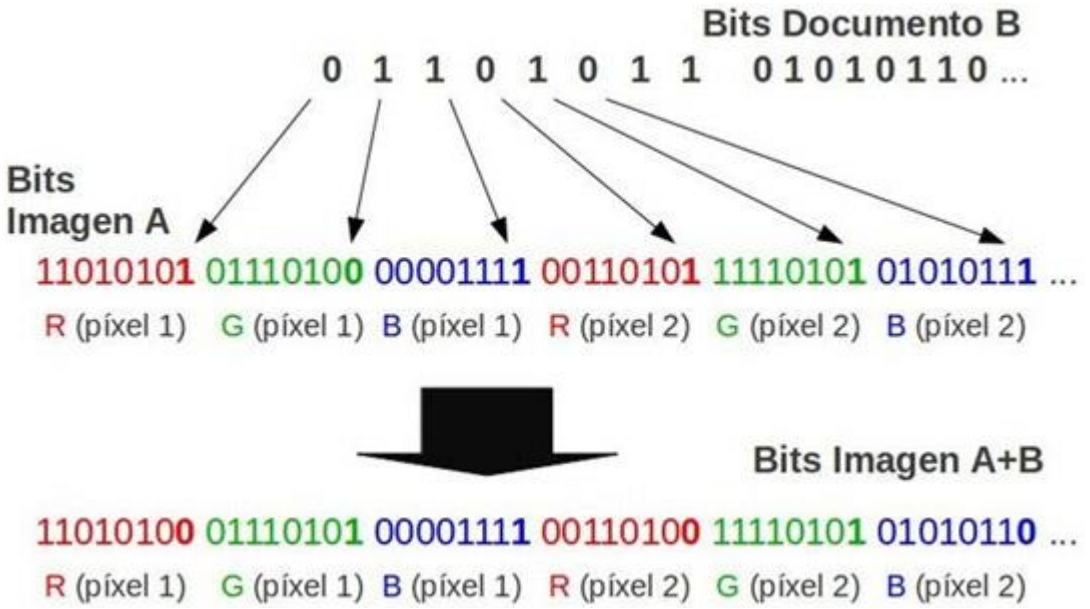
Buscar y resumir en aproximadamente media hoja las principales técnicas de esteganografía. Utilizar alguna herramienta y mostrar los pasos realizados.

La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados “portadores”, de modo que no se perciba su existencia. De este modo procura establecer un canal encubierto de comunicación. Se pueden usar muchos

formatos, pero las imágenes digitales son las más populares por su frecuencia en Internet. En este aspecto, hay diferentes técnicas cada una con sus puntos fuertes y débiles.

LSB (Least Significatn Bit)

Consiste en aprovechar el bit menos significativo de cada byte para guardar información en él. Si tenemos un texto, B, que queremos ocultar en una imagen, A, lo que hacemos es almacenar todos los bits del texto B en los bits menos significativos de cada uno de los colores que componen los píxeles de la imagen A, sustituyendo los de la propia imagen por los del documento B y añadiendo 0s una vez se ha completado el texto B. Al ser los bits que proporcionan menos información de color al píxel, los cambios realizados en los colores de la imagen no serán apreciables por el ojo humano.



Para que este método sea efectivo, la imagen no debe ser editada tras el proceso de ocultación, ya que si, por ejemplo, se comprime o se edita (se hace un crop o se rota, por ejemplo), la información de los bits cambiaría y por tanto no se podría recuperar la información ocultada. Por esto, hay que tener cuidado con los formatos que utilizan un algoritmo de compresión con pérdida, como el formato JPEG (hay variantes de JPEG que comprimen la imagen sin pérdida de datos, lossless).

Enmascaramiento y filtrado

La información se oculta dentro de una imagen digital empleando marcas de agua, teniendo como objetivo poner de manifiesto el uso no legal de un cierto servicio digital por parte de un usuario no autorizado. Otra técnica relacionada es el fingerprinting o huella digital, donde se introduce en el mensaje no sólo información sobre el autor o propietario sino además del usuario que ha adquirido los derechos de uso de ese objeto. Así se puede perseguir la distribución ilegal de servicios digitales.

Inserción de bits

Se añaden los bits de información a partir de una determinada marca estructural del fichero (fin de fichero, espacios de padding o alineamiento, etc.). El problema de esta técnica es que se incrementa el tamaño del fichero contenedor, por lo que no es muy discreta.

Referencias:
https://es.wikipedia.org/wiki/Esteganograf%C3%ADa
https://www.securityartwork.es/2013/03/07/estenografia-ocultando-el-uso-de-lsb/
https://www.securityartwork.es/2010/05/03/introduccion-a-la-esteganografia-ii/

Ejemplo de uso con Steghide:

Imagen portadora original:

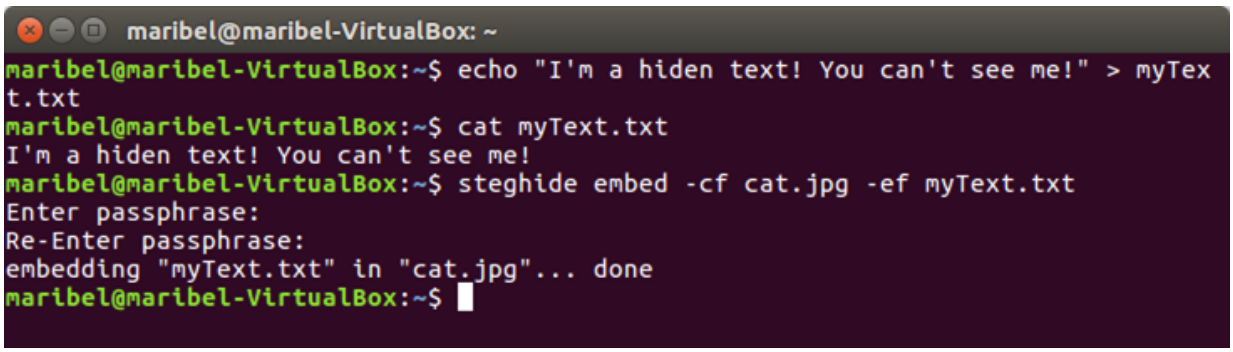
Imagen portadora modificada:

Proceso:

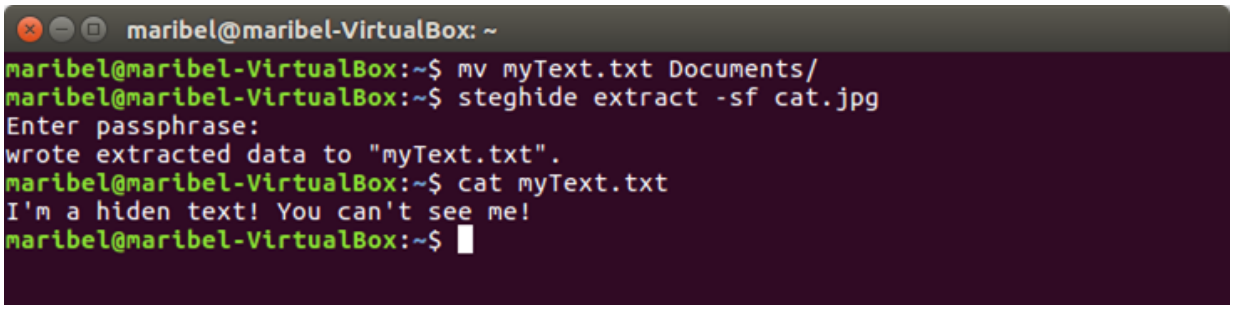
1. Instalación de Steghide:

```
maribel@maribel-VirtualBox: ~
maribel@maribel-VirtualBox:~$ sudo apt-get install steghide
[sudo] password for maribel:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libmcrypt4
Suggested packages:
  libmcrypt-dev mcrypt
The following NEW packages will be installed:
  libmcrypt4 steghide
0 upgraded, 2 newly installed, 0 to remove and 37 not upgraded.
Need to get 202 kB of archives.
After this operation, 736 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

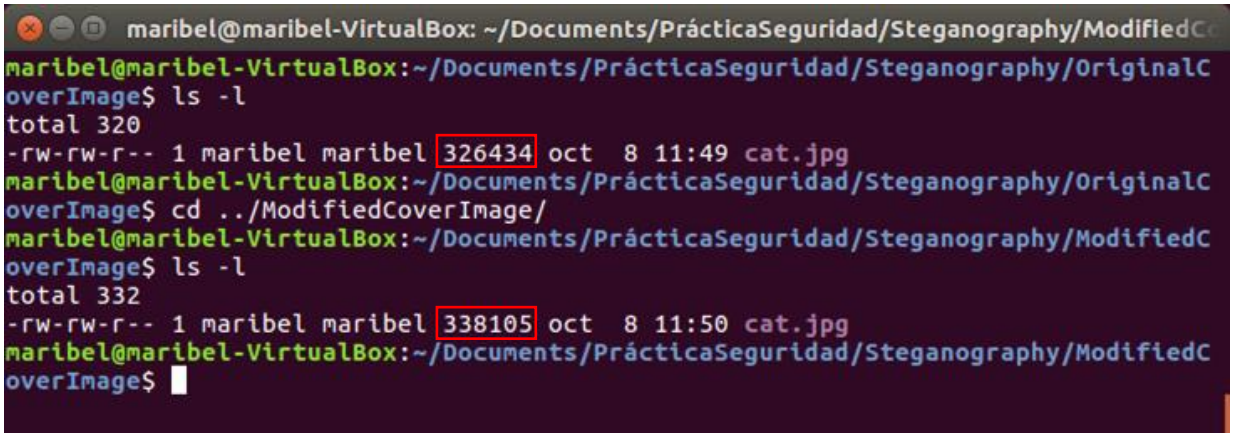
2. Ocultación de los datos (`myText.txt`) en la imagen portadora (`cat.jpg`):



3. Extracción de los datos ocultados (se mueve myText.txt de sitio para que no se sobreescriba ahora y se guarde un un archivo nuevo, para que se pueda comprobar que ha extraído los datos correctamente):



4. Comparación del tamaño de la imagen antes y después de su modificación (la imagen modificada pesa más que la original):



Referencias:
https://scottlinux.com/2014/08/12/steganography-in-linux-from-the-command-line/
https://es.wikipedia.org/wiki/Esteganograf%C3%ADa
http://www.ijaiem.org/volume3issue2/IJAIEM-2014-02-27-062.pdf

Parte 3

Analizar de forma genérica como se realiza un análisis de riesgos sobre los sistemas informáticos de una organización y exponerlo en máximo una cara.

Una adecuada gestión de los riesgos permite reducir aquellos a los que está expuesta la organización hasta unos niveles aceptables a partir de un análisis de la situación inicial. Sabremos cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenzas que podrían explotar las mismas. Podremos hacer medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Fase 1. Definir el alcance. Hay que establecer el alcance del estudio. Es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. Por ejemplo, un análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa.

Fase 2. Identificar los activos. Hacer un inventario de todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware hasta documentos escritos y los recursos humanos.

Fase 3. Identificar / seleccionar las amenazas. Identificar las amenzas a las que los activos están expuestos. Por ejemplo, si es un servidor de ficheros, podemos considerar las averías del servidor o los daños por fuego.

Fase 4. Identificar vulnerabilidades y salvaguardas. Estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, identificar un conjunto de ordenadores con un sistema operativo para el cual el desarrollador no provee soporte ni mantenimiento.

También analizaremos y documentaremos las medidas de seguridad implantadas en nuestra organización. Por ejemplo, si hemos instalada un grupo electrógeno para abastecer de electricdad a los equipos del CPD, una medida que es conocida como salvaguarda.

Fase 5. Evaluar el riesgo. Con todo lo anterior, podemos calcular el riesgo. Esta valoración suele hacerse en términos de la posibilidad de ocurrencia del riesgo y el impacto que tenga la materialización del riesgo. Para cada activo-amenaza, estimaremos la probabilidad de que la amenzada se materialice y el impacto sobre el negocio que eso produciría. Se puede hacer de modo cuantitativo (con números, como 1, 2, 3,etc) o cualitativo (con conjuntos, como Baja, Media, Alta, etc). Si hemos elegido el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto. Si hemos optado por el análisis cualitativo, usaremos una matriz de riesgo que relacione los factores probabilidad e impacto.

Fase 6. Tratar el riesgo. Debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, en un análisis cuantitativo, trataremos aquellos riestos que superen el nivel 4. Si tenemos un análisis cualitativo, trataremos aquellos riesgos que superen el nivel Medio. Podemos transferir el riesgo a un tercero, eliminarlo, asumirlo justificadamente, implantar medidas para mitigarlo.

Referencias:
https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/
https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Analizar las principales diferencias entre la ISO 27001:2005 y 27001:2013. Exponer dicha diferencia en máximo una cara.

La norma ISO 27001:2013 es la primera revisión del estándar internacional ISO 27001.

Diferencias:

- En la evaluación de riegos no requiere explícitamente la identificación de activos, amenazas y vulnerabilidades como prerrequisitos para la identificación de riesgos.
- También utiliza el vocabulario de ISO 31000 y, por lo tanto, la norma ISO 27001:2013 se refiere a las consecuencias más que a los impactos.

- Control documental: no se requerirán cambios a los procedimientos documentados existentes en materia de control de documentación.
- Auditoría interna: no serán necesarios cambio a los procedimientos de documentación existente relacionados con auditoría interna.
- Acciones correctivas: los procedimientos existentes pueden necesitar ser reforzados para asegurarse de que se reaccione ante las no conformidades y se tome acción, como aplica, controlarlos y corregirlos y trabajar con las consecuencias.
- Mejora: asegura que existen procedimientos para la mejora continua que se extienden para cubrir la idoneidad y adecuación de un SGSI así como su efectividad.

Referencias:
http://www.pmg-ssi.com/2015/02/comparativa-entre-la-iso-270012013-y-la-iso-270012005/
https://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf

Analizar las diferentes fases de la metodología OWASP y resumirlas en máximo una cara.

Son técnicas y tareas que son apropiadas en varias fases del ciclo de vida de desarrollo de software. Este modelo no es obligatorio, pero es una aproximación flexible que puede ser adaptada a cada organización.

- **Fase 1. Antes de comenzar el desarrollo**
  - **Fase 1.1. Definir un ciclo de desarrollo de software**
    Establecer un ciclo de desarrollo de software adecuado donde la seguridad se tiene en cuenta en cada etapa.
  - **Fase 1.2. Políticas de revisión y estándares**
  - Asegurarse de que las políticas, estándares y documentación adecuados están en su sitio. Son muy importantes, ya que sirven de guías a los desarrolladores. Por ejemplo, si una aplicación se va a desarrollar en Java, es esencial que haya un estándar de codificación seguro. Si se va a utilizar criptografía, que haya un estándar de criptografía. No todas las situaciones se pueden documentar, pero hacerlo con los problemas más probables implicará menos toma de decisiones durante el proceso de desarrollo.
  - **Fase 1.3. Métricas**
  - Definir el criterio que necesita ser medido provee visibilidad a los defectos tanto en el proceso y en el producto.

- **Fase 2. Durante la definición y el diseño**
  - **Fase 2.1. Repasar requisitos de seguridad**
  - Mirar si hay faltas (gaps) en las definiciones de los requisitos. Por ejemplo, en los siguientes campos: administración de usuarios, autenticación, autorización, confidencialidad de los datos, integridad, etc.
  - **Fase 2.2. Repaso del diseño y la arquitectura**
  - Esta documentación puede incluir modelos, documentos textuales y artefactos similares. Es esencial asegurar que el diseño y la arquitectura tienen el nivel de seguridad definido en los requisitos. Por ejemplo: si puedes ser autorizado en varios sitios de la página, se puede pensar en un componente de autorización central.
  - **Fase 2.3. Crear y revisar modelos UML**
  - Una vez que el diseño y la arquitectura están preparado, construir un modelo UML que describa cómo funciona la aplicación.
  - **Fase 2.4. Crear y repasar modelos de amenaza**
  - Analizar el diseño y la arquitectura para asegurar que las amenazas han sido mitigadas, aceptadas por la organización o asignadas a un tercero.

- **Fase 3. Durante el desarrollo**
  - **Fase 3.1. Walk through por el código**

    - El propósito no es hacer una code review, sino entender a un alto nivel el flujo, la composición y la estructura del código que compone la aplicación.
    - **Fase 3.2. Code reviews**
    - Una vez que se entiende bien cómo está estructurado el código y por qué ciertas cosas fueron codificadas de una manera, podemos examinar el código para buscar defectos de seguridad. Por ejemplo: Los requisitos de disponibilidad, confidencialidad e integridad de la organización; las exposiciones técnicas de la guía OWASP, problemas específicos relacionados con el lenguaje o framework que se está usando, etc.

- **Fase 4. Durante el despliegue**
    - **Fase 4.1. Application Penetration Testing**
    - Habiendo probado los requisitos, analizado el diseño, y realizada la code review, puede que se asuma que todos los problemas están controlados. Pero penetration testing la aplicación después de que haya sido desplegada no es mala idea.
    - **Fase 2.1. Configuration Management Testing**
    - La penetration test de la aplicación debería incluir la comprobación de cómo se desplegó y aseguró la infraestructura. Mientras que la aplicación a lo mejor es segura, un pequeño aspecto de la configuración puede que esté todavía en una etapa de instalación por defecto y vulnerable a la explotación.

- **Fase 5. Mantenimiento y operaciones**
    - **Fase 5.1. Dirigir Operational Management Reviews**
    - Es necesario que haya un proceso que detalle cómo se administra el lado operacional de la aplicación y la infraestructura.
    - **Fase 5.2. Dirigir comprobaciones periódicas de salud**
    - Comprobaciones mensuales o cuatrimestrales sobre la aplicación y la estructura para asegurar de que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue todavía intacto.
    - **Fase 5.3. Asegurar la verificación de los cambios**
    - Después de que cada cambio ha sido aprobado y probado en el entorno QA y desplegado al entorno de aplicación, es vital que el cambio sea comprobado para asegurar que el nivel de seguridad no ha sido afectado por el cambio. Esto debería estar integrado en el proceso de administración de los cambios.

Referencia:
https://www.owasp.org/index.php/The_OWASP_Testing_Framework