

INTRODUCCION A LA SEGURIDAD INFORMATICA

Practica 1 TEMAS 1,2,3,4



Ramón Rojas Soto

1. Ataques entre los años 2019/2020



2019

- **Método de ataque:** El hacker aprovechó la vulnerabilidad denominada **Server Side Request Forgery** (SSRF) en la que se puede engañar a un servidor para que ejecute comandos que nunca se le debería haber permitido ejecutar. Escaneo los clientes de la nube en busca de una configuración incorrecta del firewall de aplicaciones web específicas en este caso AWS, a partir de aquí explotó para extraer credenciales de cuentas privilegiadas para bases de datos y otras aplicaciones web.
- **Objetivos del ataque:** El hacker comprometió aproximadamente 140,000 números de la Seguridad Social y aproximadamente 80,000 números de cuentas bancarias de clientes estadounidenses y 1 millón de números de Seguridad Social (SIN) de clientes de tarjetas de crédito canadienses, además de un número no revelado de nombres de personas, direcciones, aval crediticio, límites de crédito, saldos y otra información. En total, el incidente afectó a aproximadamente 100 millones de personas en los Estados Unidos y seis millones en Canadá.
- **Países afectados:** Estados Unidos y Canadá.
- **Tiempo de actividad:** Capital One dice que empezó entre el 22 y el 23 de marzo, el 17 de Julio informan a la empresa de que sus datos están siendo compartidos en Github y el 29 de Julio detienen al hacker.



2019

- **Método de ataque:** Los atacantes obtuvieron acceso ilícito al sitio web de AMCA y ejecutaron un ataque **Man-in-the-Middle** (MITM) que se centró en las páginas web que se ocupaban de los pagos de todas las partes interesadas.

- **Objetivos del ataque:** Los atacantes registraron el pago y la información personal ingresada por los visitantes de Quest como registros médicos internos (como los resultados de las pruebas de laboratorio). La brecha afectó a 11,9 millones de clientes. La información expuesta incluye números de tarjetas de crédito, información de cuentas bancarias, datos médicos, identidad personal y datos de contacto, incluidos los números de seguro social.
- **Países afectados:** Estados Unidos
- **Tiempo de actividad:** La violación se remonta al 1 de agosto de 2018 hasta el 30 de marzo de 2019, pero AMCA la descubrió el 14 de mayo de 2019 e informó a Quest.

2. Acciones y programas de espionaje de la NSA

Para poder llevar a cabo esta ingente labor, la NSA –que desde 2009 comparte jefatura con el mando militar del ciberespacio (US Cyber Command, USCYBERCOM) que, dependiente del mando estratégico estadounidense, se encarga de realizar operaciones en este nuevo dominio.

Programas revelados:

Quantum y Foxacid : Programas de ataques selectivos contra usuarios de TOR, según mostraban los documentos filtrados sobre su funcionamiento publicados el 4 de octubre. El modo en que operaban se basaba no tanto en atacar a la propia red TOR como a los sistemas de los usuarios que accedían a ella, según explicaba para The Guardian Bruce Schneier, experto en seguridad informática.

Tras identificar un usuario de TOR, “la NSA utiliza su red de servidores secretos de internet para redirigir los usuarios a otro conjunto de servidores secretos de internet, con el nombre en clave FOXACID, para infectar el ordenador del usuario”. Para ejecutar este ataque, la NSA se serviría de unos servidores secretos de alta velocidad denominados QUANTUM.

Tempora: Programa de la agencia de inteligencia británica GCHQ para el acceso a redes informáticas y telefónicas, y a datos de localización, así como a algunos sistemas. Fue destapado por The Guardian el 21 de julio.

El GCHQ tiene acceso a la red de cables que transportan llamadas telefónicas y el tráfico de internet de todo el mundo, y ha comenzado a procesar grandes flujos de información personal sensible que está compartiendo con su socio estadounidense, la Agencia Nacional de Seguridad (NSA). Almacenan grandes volúmenes de datos procedentes de cables de fibra óptica hasta 30 días para que pueda ser filtrada y analizada.

Esa operación, cuyo nombre en código es TEMPORA, ha estado funcionando durante unos 18 meses. En mayo del año pasado, 300 analistas de GCHQ y 250 de la NSA habían sido asignados para procesar la inundación de datos capturada.

Prism: Programa de la Agencia Nacional de Seguridad estadounidense (NSA), operativo desde 2007, que permite la vigilancia masiva de ciudadanos de la UE mediante un acceso directo a los servidores centrales de empresas estadounidenses líderes en internet, como Google, Microsoft, Facebook, Yahoo, Skype o Apple. La cantidad y modalidad de los datos aportados varía según la compañía.

El programa PRISM (o “Prisma”, es español) permite el acceso de los servicios de espionaje a información masiva muy variada. Según se recoge en el Power Point filtrado con el que la propia NSA explicaba su funcionamiento, es capaz de obtener historial de búsquedas, contenido de correos electrónicos, transferencia de archivos, chats, fotografías, videoconferencias o registros de conexiones.

Esta recogida masiva e indiscriminada de información se realiza bajo la supuesta cobertura legal de la Ley Patriótica (Patriot Act), aprobada por el Congreso estadounidense tras los ataques del 11 de septiembre, y, sobre todo, de la Ley de vigilancia de extranjeros o FISA (Foreign Intelligence Surveillance Act), una norma de 1978 enmendada en numerosas ocasiones (la última vez en 2008). Esta ley establece un tribunal secreto (FISA Court), que es el que autoriza las operaciones de rastreo emprendidas por la NSA.

Xkeyscore: Dado a conocer por O Globo y Der Spiegel el 20 de julio, se trata de un programa dedicado a la búsqueda y análisis del contenido y los metadatos de nuestras comunicaciones online. Tiene la capacidad de acceder, sin ningún tipo de autorización previa, a prácticamente cualquier actividad del usuario típico de internet, según destacaba una de las diapositivas publicadas, orientadas a la formación de los analistas.

El propósito de XKEYSCORE, según explicaba unos días después The Guardian, es “permitir a los analistas buscar tanto en los metadatos como en el contenido de los correos electrónicos y otras actividades de internet”, como búsquedas, conversaciones en redes sociales o el historial de navegación. Y todo ello con un procedimiento tan sencillo como rellenar en el sistema un formulario que no exige justificar la búsqueda, incluso cuando no se parte de una cuenta de correo electrónico conocida.

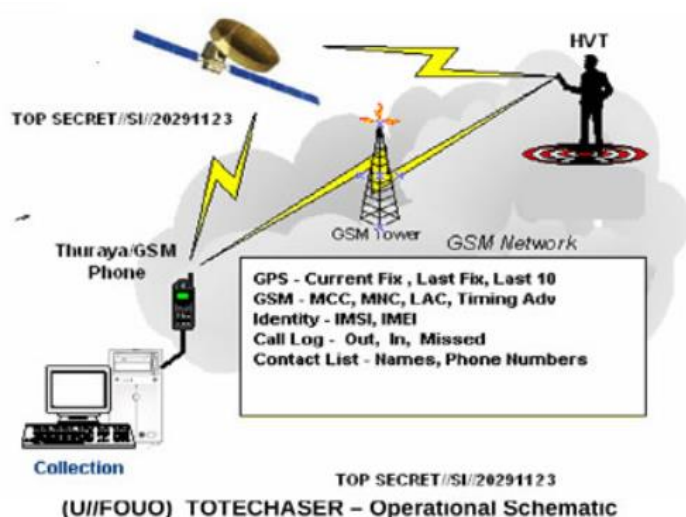
Las búsquedas se pueden efectuar a partir del nombre, el número de teléfono, la dirección IP, palabras clave, el idioma o el tipo de navegador utilizado. Otra de las diapositivas muestra cómo la actividad de internet está continuamente siendo recogida por XKEYSCORE y el analista tiene capacidad para consultar las bases de datos en cualquier momento.

3. Proyectos del catálogo ANT TAO

TOTECHASER: Es un implante escondido en el Flashrom del teléfono satelital Thuraya 2520 que pasa los datos en Windows CE incorporado y se transmiten a través de mensajes de texto SMS ocultos.

Las capacidades iniciales de implantación de software incluyen proporcionar información de geolocalización GPS y GSM. El registro de llamadas, la lista de contactos y otra información del usuario también se pueden recuperar del teléfono. Se están investigando capacidades adicionales.

TOTECHASER utilizará mensajería SMS para la ruta de comando, control y exfiltración de datos. La capacidad inicial utilizará mensajes SMS encubiertos para comunicarse con el teléfono. Estos mensajes encubiertos se pueden transmitir en modo Thuraya Satellite o en modo GSM y no alertarán al usuario de esta actividad. Un canal de comando y control alternativo que utiliza la conexión de datos GPRS basada en el implante TOTEHOSTLY está previsto para una versión futura.



GENESIS: Es un teléfono móvil normal, modificado para GSM y 3G que puede determinar los parámetros de red y el uso del espectro, así como localizar otros teléfonos móviles.

Los sistemas GENESIS están diseñados para soportar operaciones encubiertas en entornos hostiles. Un usuario inteligente podría estudiar el entorno local con la herramienta analizadora de espectro, seleccionar el espectro de interés para registrar y descargar la información del espectro a través de Ethernet integrado a un controlador de computadora portátil. El sistema GENESIS también podría utilizarse, junto con un interrogador activo, como herramienta de acabado cuando se realizan operaciones de Buscar / Reparar / Finalizar en entornos no convencionales.

Características:

- SDR oculto con interfaz de menú de auricular
- Capacidad del analizador de espectro
- Capacidad de búsqueda / reparación / acabado
- Ethernet integrado
- Puerto de antena externa
- 16 GB de almacenamiento interno
- Varias antenas integradas



(S//SI//REL) GENESIS Handset

4. Uso de TOR para acceder a la Deep Web

Accedemos a TOR y por defecto nos viene configurado **DuckDuckGo**, con una simple búsqueda de buscadores de Deep web aparecen todos los que tiene.

This list contains the search engines most requested by the community on the deep web.

- <http://3g2upl4pg6kufc4m.onion> – **DuckDuckGo** – For the darknet, but searches only the clearnet.
- <http://hss3uro2hsxfogfq.onion> – **not Evil** – The premier search engine of onionland.
- <http://visitorfi5kl7q7l.onion> – **visitor** – Evil and clone domains filtered. Good accuracy.
- <http://msydgstlz2kzerdg.onion> – **Ahmia.fi** – onion and tor2web search links. Reasonable accuracy.
- <http://xmh57jrzrnw6insl.onion> – **Torch** – onion searches. Poor search-result accuracy.
- <http://7pwy57lklv6lyhe.onion> – **Dark Search Engine** - A new search engine for the darknet.
- <http://bzjltqphs2lp4xdd.onion> – **Dark web links** – A new search engine. Poor result accuracy.
- <http://searchb5a7tmimez.onion> – **searx** – Search engine for the clearnet. Categories.
- <http://gjobqij7wyczbqie.onion> – **Candle** – Retro-like-design. Fine search-result accuracy.
- <http://kbhpodhnfxl3clb4.onion> – **TorSearch** – Around 410K .onion pages indexed currently.
- <http://carontevaha5x626.onion> – **Caronte** – A new search engine with good accuracy.

Buscamos links interesantes en el Hidden Wiki

Email and Messaging

- <http://bitmailendavkbec.onion> – swiss email
- <http://365u4bxqfy72nul.onion/> – Anonymous E-mail service. You can only communicate with other users currently using this service. So tell all your friends about it!
- <http://sms4tor3vcr2geip.onion/> – SMS4TOR – Self destructing messages
- <http://notestjxctkwbk6z.onion/> – NoteBin – Create encrypted self-destructing notes
- <http://torbox3uiot6wchz.onion/> – [TorBox] The Tor Mail Box
- <http://u6lyst27lmelm6oy.onion/index.php> – Blue matrix chat NOT UP ALL THE TIME so chek often to see when it is
- <http://wi7qloxyrdpu5cmvr.onion/> – Autistici/Inventati
- <http://u4uoz3aphqbdq754.onion/> – Hell Online

Political

- http://6sgjmi53igm7fm7.onion/index.php?title=Main_Page – Bugged Planet
- <http://faerieuaahqvzgbby.onion/> – Fairie Underground

Y en el primero de la sección “Political” tenemos información recopilada sobre seguridad de España

SIGINT/COMINT Stations and Operators

Name	Location	Operator	Capabilities
	Pico de las Nieves, Grand Canary Island	ES-operated "accommodation site" that provides occasional SIGINT product to the US INSCOM	
	Manzanares	ES-operated "accommodation site" that provides occasional SIGINT product to the US INSCOM	
	Playa de Pals	Contractor-operated US facility.	
Naval Station Rota Spain	Rota (36°37'15"N 6°19'54"W)		

Privacy Related Legislation

LI Legislation

SIGINT/COMINT Legal Grounds

Vendor Appearance

- Vendor with Place of Registration in Spain: [AGNITIO](#)
- 2013: [HACKINGTEAM](#) see [securelist.com](#) Report 20130425

5. Tipos de denegaciones de servicio

Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.

Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática

Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (Denial of Service) y la denegación de servicio distribuido o DDoS (Distributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP's que realizan el ataque.

Ataques DDoS populares:

UDP Flood (Saturación UDP): 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.

Service Port Flood (Ataque sobre Puertos de Servicio): Así como en los ataques UDP Flood se atacaban puertos aleatoriamente, en este tipo de ataques las peticiones irán dirigidas hacia los puertos estándar en los que se conoce que habrá más volumen de tráfico (el puerto TCP 80, por ejemplo) tanto entrante como saliente.

SYN Flood: Así funciona la secuencia de conexión de tres pasos del protocolo SYN. Nosotros enviamos una petición SYN para iniciar la conexión TCP que el host al que conectamos debe responder con un paquete SYN-ACK para nosotros confirmarlo con una respuesta ACK. El ataque comienza cuando ignoramos la petición ACK por parte de nuestro objetivo, este mantiene las conexiones abiertas a la espera de respuesta y nosotros continuamos enviando

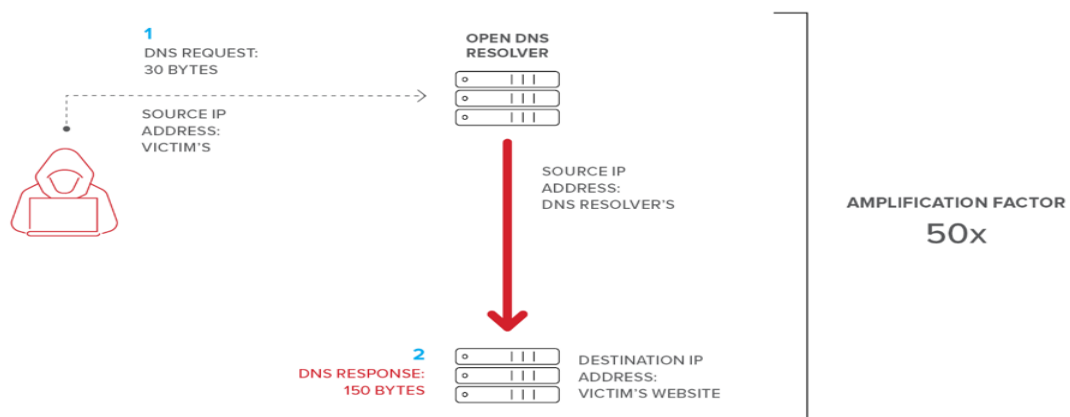
paquetes SYN, lo que provoca que dicha máquina siga enviando peticiones SYN-ACK; saturando así el tráfico saliente y entrante del host

Ping of Death (Ping 'de la Muerte'): Por norma general una petición ping tiene un tamaño de 32 bytes (incluida la cabecera) y los servidores no tienen ningún problema para gestionar las peticiones y enviar la respuesta correspondiente legítimas.

Con el conocido como "Ping de la muerte" (Ping of Death o PoD), lo que hacemos es enviar paquetes mediante ping, pero con un tamaño mucho mayor y a mayor frecuencia de lo normal.

Ataque DDoS por ampliación

Un ataque de ampliación del servidor de nombres de dominio (DNS) es una forma popular de denegación de servicio distribuida (DDoS), en la que los atacantes utilizan servidores DNS abiertos de acceso público para inundar un sistema objetivo con tráfico de respuesta DNS. La técnica principal consiste en que un atacante envíe una solicitud de búsqueda de nombre DNS a un servidor DNS abierto con la dirección de origen falsificada para que sea la dirección del objetivo. Cuando el servidor DNS envía la respuesta del registro DNS, se envía en su lugar al destino. Los atacantes suelen enviar una solicitud de tanta información de zona como sea posible para maximizar el efecto de ampliación. En la mayoría de los ataques de este tipo observados, las consultas falsificadas enviadas por el atacante son del tipo "CUALQUIERA", que devuelve toda la información conocida sobre una zona DNS en una sola solicitud.



Practica 1 - TEMA 2

1. Herramientas para desplegar un Honeypot

Database Honeypots:

- Elastic honey - A Simple Elasticsearch Honeypot
- ESPot - ElasticSearch Honeypot

Web honeypots

- Glastopf - Web Application Honeypot
- servlet - Web application Honeypot
- Nodepot - A nodejs web application honeypot
- Shadow Daemon - A modular Web Application Firewall / High-Interaction Honeypot for PHP, Perl & Python apps

Service Honeypots

- Kippo - Medium interaction SSH honeypot
- honeyntp - NTP logger/honeypot
- Ensnare - Easy to deploy Ruby honeypot

ICS/SCADA honeypots

- Conpot - ICS/SCADA honeypot
- SCADA honeynet - Building Honeypots for Industrial Networks

Server

- LaBrea - takes over unused IP addresses, and creates virtual servers that are attractive to worms, hackers, and other denizens of the Internet.
- Kippo - SSH honeypot
- KFSensor - Windows based honeypot Intrusion Detection System (IDS)

Desplegar un Honeypot:

1. Instalar Docker

- Añadir la clave GPG oficial

```
usuario1@usuario1-VirtualBox:~$ sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
OK
usuario1@usuario1-VirtualBox:~$ sudo apt-key fingerprint 0EBFCD88
pub   rsa4096 2017-02-22 [SCEA]
      9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid           [ unknown] Docker Release (CE deb) <docker@docker.com>
sub   rsa4096 2017-02-22 [S]
```

- Descargar el repositorio estable: **sudo add-apt-repository \ "deb [arch=amd64] <https://download.docker.com/linux/ubuntu> \ \$(lsb_release -cs) \ stable"**

```
usuario1@usuario1-VirtualBox:~$ sudo add-apt-repository \
> "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
> $(lsb_release -cs) \
> stable"
Get:1 https://download.docker.com/linux/ubuntu bionic InRelease [64,4 kB]
Hit:2 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:3 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Get:4 https://download.docker.com/linux/ubuntu bionic/stable amd64 Packages [13,
0 kB]
Hit:5 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:6 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease
Fetched 77,4 kB in 1s (130 kB/s)
Reading package lists... Done
```

- Instalamos la última versión de Docker engine: **sudo apt-get install docker-ce docker-ce-cli containerd.io**

```
usuario1@usuario1-VirtualBox:~$ sudo apt-get install docker-ce docker-ce-cli con
tainerd.io
Reading package lists... Done
```

- Por último comprobamos que todo está correcto: **sudo docker run hello-world**

```
usuario1@usuario1-VirtualBox:~$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
0e03bdcc26d7: Pull complete
Digest: sha256:8c5aeeb6a5f3ba4883347d3747a7249f491766ca1caa47e5da5dfcf6b9b717c0
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

- Instalamos Docker-compose (por si lo necesitamos también para cargar conpot)

```
usuario1@usuario1-VirtualBox:~/conpot/docker$ docker-compose --version
docker-compose version 1.27.4, build 40524192
usuario1@usuario1-VirtualBox:~/conpot/docker$
```

2. Desplegar Conpot

- Nos descargamos conpot desde el repositorio oficial de GitHub: **git clone <https://github.com/mushorg/conpot.git>**

```

usuario1@usuario1-VirtualBox:~$ git clone https://github.com/mushorg/conpot.git
Cloning into 'conpot'...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 8260 (delta 8), reused 2 (delta 2), pack-reused 8235
Receiving objects: 100% (8260/8260), 2.72 MiB | 4.69 MiB/s, done.
Resolving deltas: 100% (5601/5601), done.
usuario1@usuario1-VirtualBox:~$ cd conpot/docker/

```

- Arrancamos Docker con conpot: `docker run -it -p 80:80 -p 102:102 -p 502:502 -p 161:161/udp --network=bridge honeynet/conpot:latest /bin/sh`

```

usuario1@usuario1-VirtualBox:~/conpot/docker$ sudo docker run -it -p 80:80 -p 102:102 -p 502:502 -p 161:161/udp --network=bridge honeynet/conpot:latest /bin/sh
~ $ conpot -f --template default
/bin/sh: conpot: not found
~ $ conpot --template default
/bin/sh: conpot: not found
~ $

```

```

usuario1@usuario1-VirtualBox:~/conpot/conpot/templates$ ls
default guardian_ast IEC104 ipmi kamstrup_382 proxy
usuario1@usuario1-VirtualBox:~/conpot/conpot/templates$

```

FALLOS: Con lo anterior debería funcionar sin ningún problema, en mi caso ya no se que mas hacer, arrancando con Docker normal no me reconoce conpot por lo tanto no lo arranca ni nada, pero se ven en las imágenes anteriores que están los archivos y que están cargados.

Por otro lado he intentado montarlo con Docker-compose que es otra forma de montar Docker pero debo de tener algún fallo con los ficheros de Python que no consigue encontrar alguna dependencia.

```

>
      metadata, options = get_config()
      File "/tmp/pip-install-dzba4uf0/mysqlclient/setup_posix.py", line 65, in g
et_config
        libs = mysql_config("libs")
      File "/tmp/pip-install-dzba4uf0/mysqlclient/setup_posix.py", line 31, in m
ysql_config
        raise OSError("{} not found".format(_mysql_config_path))
      OSError: mysql_config not found

-----
Command "python setup.py egg_info" failed with error code 1 in /tmp/pip-install-
dzba4uf0/mysqlclient/
You are using pip version 18.1, however version 20.2.4 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
ERROR: Service 'conpot' failed to build : The command '/bin/sh -c pip3 install -
-user --no-cache-dir -r requirements.txt' returned a non-zero code: 1

```

2. Analizar uso de Snort y desplegarlo como IDS

Snort es un Sistema de Detección de Intrusos (IDS) basado en red (IDSN) open source . Cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se

utilizarán a la hora de monitorizar el sistema. Además, ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que se adapte lo máximo posible a lo que deseamos.

Una de las ventajas de este sistema es que puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se loguea. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

1.Instalar SNORT(seguiamos los pasos del recurso)

- Descargamos el fichero comprimido desde la pagina de Snort y lo guardamos en la carpeta que nos hemos creado, a continuación lo descomprimimos y lo instalamos con el comando: **./configure && make && sudo make install**

```
lecikt@kali:~/snort_source$ ls
snort-2.9.16.1  snort-2.9.16.1.tar.gz
lecikt@kali:~/snort_source$ cd snort-2.9.16.1/
lecikt@kali:~/snort_source/snort-2.9.16.1$ ls
aclocal.m4  compile  config.h.in  configure  COPYING  doc  install-sh  ltmain.sh  Makefile.am  missing  RELEASE.NOTES  snort.8  src  tools
ChangeLog  config.guess  config.sub  configure.in  depcomp  etc  LICENSE  m4  Makefile.in  preproc_rules  rpm  snort.pc.in  templates  VERSION
```

- Al instalarlo nos aparece un error sobre el paquete lib, nos descargamos el fichero desde la pagina lo metemos en nuestra carpeta y lo descomprimimos **tar -xvzf libpcap-1.9.1.tar.gz** para instalarlo a continuación : **./configure && make && sudo make install**
- Seguimos descargando paquetes descomprimiéndolos e instalándolos, al final nuestro directorio debe quedar así

```
lecikt@kali:~/snort_source$ ls -l
total 10736
drwxr-xr-x 13   179 snort    12288 oct 25 18:22 libpcap-1.9.1
-rw-r--r--  1 lecikt lecikt  861228 oct 25 18:20 libpcap-1.9.1.tar.gz
drwxr-xr-x  6   lecikt lecikt   4096 may  1 2017 LuaJIT-2.0.5
-rw-r--r--  1 lecikt lecikt  849845 oct 25 18:36 LuaJIT-2.0.5.tar.gz
drwxr-xr-x  7   1169 1169    4096 oct 25 18:36 pcre2-10.35
-rw-r--r--  1 lecikt lecikt 2299082 oct 25 18:31 pcre2-10.35.tar.gz
drwxrwxr-x 10   lecikt lecikt   4096 oct 25 18:40 snort-2.9.16.1
-rw-r--r--  1 lecikt lecikt 6947960 oct 25 18:08 snort-2.9.16.1.tar.gz
```

- Una vez terminada la guía comprobamos con **snort -V** si esta todo correcto, en mi caso no lo está. A continuación hay varias imágenes de los errores encontrados durante la instalación de los diferentes paquetes. Creo que es de mi propia instalación de Kali

```
Mensajes del ensamblador:
Error fatal: no se puede crear pcap-linux.o: Permiso denegado
make: *** [Makefile:87: pcap-linux.o] Error 1
```

```
rm -f src/pcr2_chartables.c
ln -s /home/lecikt/snort_source/pcr2-10.35/src/pcr2_chartables.c.dist /home/lecikt/snort_source/pcr2-10.35/src/pcr2_chartables.c
ln: fallo al crear el enlace simbólico '/home/lecikt/snort_source/pcr2-10.35/src/pcr2_chartables.c': Permiso denegado
make: *** [Makefile:3586: src/pcr2_chartables.c] Error 1
```

```
lecikt@kali:~/snort_source/snort-2.9.16.1$ sudo ./configure --enable-sourcefire && make && sudo make install
configure: WARNING: you should use --build, --host, --target
configure: WARNING: invalid host type: -
configure: WARNING: you should use --build, --host, --target
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for --gcc... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
checking for --gcc... gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking whether gcc understands -c and -o together... (cached) yes
checking dependency style of gcc... (cached) gcc3
checking build system type... Invalid configuration '-': machine '-' not recognized
configure: error: /bin/bash ./config.sub - failed
lecikt@kali:~/snort_source/snort-2.9.16.1$ snort -V
bash: snort: orden no encontrada
lecikt@kali:~/snort_source/snort-2.9.16.1$
```

Las reglas o firmas son los patrones que se buscan dentro de los paquetes de datos. Las reglas de Snort son utilizadas por el motor de detección para comparar los paquetes recibidos y generar las alertas en caso de existir coincidencia entre el contenido de los paquetes y las firmas. El archivo **/etc/snort/snort.conf**. En mi caso como no las tengo me he descargado las reglas de la comunidad de la propia página de Snort

```
lecikt@kali:~/snort_source/community-rules$ ls
AUTHORS  community.rules  LICENSE  sid-msg.map  snort.conf  VRT-License.txt
```

Un par de reglas , una alerta TCP por si alguien intenta un XMKD overflow a través de FTP

```
# alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"PROTOCOL-FTP XMKD overflow attempt"; flow:to_server,established;
# alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"PROTOCOL-FTP NLST overflow attempt"; flow:to_server,established;
```

La ultima que es una alerta sobre inyección de código

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Silence variant outbound conn
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Silence variant outbound conn
alert tcp $HOME_NET any -> $EXTERNAL_NET [$HTTP_PORTS,10011] (msg:"MALWARE-CNC Andr.Trojan.Moonshine outbound c
# alert udp any 67 -> $HOME_NET 68 (msg:"OS-LINUX Red Hat NetworkManager DHCP client command injection attempt"
```

3. MDM en la actualidad dentro de una organización

Mobile Device Management es la gestión de los dispositivos móviles en el ámbito de las empresas. O exactamente, un software que permite administrar de forma segura los smartphones, tablets, portátiles, impresoras móviles. Una plataforma que admita cualquier operador de telefonía y servicios, y que garantice el uso seguro de los equipos, tanto propios de la empresa como aportados por sus trabajadores (BYOD).













Su cometido es:







- Rastrear equipos conectados
- Gestionar la descarga de aplicaciones
- Optimizar el funcionamiento de los dispositivos móviles, reduciendo costes y tiempos de configuración
- Controlar y proteger los datos
- Delimitar el alcance de la navegación y usos de las aplicaciones
- Monitorizar el funcionamiento de la red móvil
- Detectar fallos y repararlos
- Sincronizar ficheros
- Administrar contraseñas
- Bloquear funciones, como son la cámara, el micrófono, el USB o los ajustes de los dispositivos
- Borrar datos de los dispositivos, en caso de pérdida o robo

Fabricante/Proveedor: ManageEngine

Software: Mobile Device Manager Plus

Esta empresa cumple con todos los requisitos que se piden a un MDM es una herramienta muy completa

 Device Management	 App Management	 Security Management	 Email Management	 Content Management	 Containerization
 Device Enrollment Enroll devices manually, in bulk or make users' self-enroll their iOS or Android devices with two factor authentication.	 App Management Install in-house and store apps silently, create your own app catalog, restrict blocklisted apps and more.	 Profile Management Create and configure policies and profiles for different departments/roles and associate them with appropriate groups.			
 Email Management Manage and secure corporate emails through Platform Containerization and Exchange ActiveSync.	 Kiosk Mode Restrict your device to access a single or a specific set of apps.	 Remote Troubleshooting Remotely view and control mobile devices. Solve device related issues in real time.			

 Asset Management Scan to fetch the details of installed apps, enforced restrictions, installed certificates and device hardware details.	 Security Management Configure stringent security policies such as the passcode, device lock to protect corporate data from outside threats.	 Content Management Remotely share documents to the devices over-the-air. Securely save and view documents on the devices.
 Audit and Reports Audit mobile devices with out-of-the-box reports such as Rooted Devices, Devices with Blocklist Apps, etc.	 Rugged Device Management Complete lifecycle management of ruggedized laptops and handhelds.	 Integrations Manage devices from a unified console by integrating with other business essential applications.

Practica 1 - TEMA 3

1. Mitre ATT&CK CVSS

Grupo Cybercriminal: Carbanak

Técnicas:

- Create or Modify System Process:** Los adversarios pueden crear o modificar procesos a nivel del sistema para ejecutar repetidamente payloads maliciosos como parte de la persistencia. Cuando los sistemas operativos se inician, pueden iniciar procesos que realizan funciones del sistema en segundo plano.
- Impair Defenses:** Los adversarios pueden modificar maliciosamente componentes del entorno de una víctima para obstaculizar o deshabilitar los mecanismos defensivos. Esto no solo implica perjudicar las defensas preventivas, como firewalls y antivirus, sino también capacidades de detección que los defensores pueden usar para auditar la actividad e identificar comportamientos maliciosos.
- Signed Binary Proxy Execution:** Los adversarios pueden eludir las defensas basadas en firmas y / o procesos mediante el proxy de ejecución de contenido malicioso con binarios firmados. Los binarios firmados con certificados digitales confiables pueden ejecutarse en sistemas Windows protegidos por validación de firma digital.
- Web Service:** Los adversarios pueden utilizar un servicio web externo legítimo existente como un medio para transmitir datos hacia / desde un sistema comprometido. Los sitios web populares y las redes sociales que actúan como un mecanismo para C2 pueden brindar una cobertura significativa debido a la probabilidad de que los hosts dentro de una red ya se estén comunicando con ellos antes de un compromiso.

Grupo Cybercriminal: Blue Mockingbird

Técnicas:

- **Access Token Manipulation:** Los adversarios pueden modificar los tokens de acceso para operar bajo un contexto de seguridad de sistema o usuario diferente para realizar acciones y evitar los controles de acceso. Windows usa tokens de acceso para determinar la propiedad de un proceso en ejecución. Un usuario puede manipular los tokens de acceso para hacer que un proceso en ejecución parezca hijo de un proceso diferente o pertenezca a otra persona que no sea el usuario que inició el proceso.
- **Exploit Public-Facing Application:** Los adversarios pueden intentar aprovecharse de una debilidad en una computadora o programa conectado a Internet utilizando software, datos o comandos para causar un comportamiento no intencionado o no anticipado. La debilidad del sistema puede ser un error, una falla o una vulnerabilidad de diseño.
- **Hijack Execution Flow:** Los adversarios pueden ejecutar sus propias cargas maliciosas al secuestrar la forma en que los sistemas operativos ejecutan los programas. El flujo de ejecución secuestrado puede ser con fines de persistencia, ya que esta ejecución secuestrada puede volver a ocurrir con el tiempo. Los adversarios también pueden usar estos mecanismos para elevar privilegios o evadir defensas, como el control de aplicaciones u otras restricciones de ejecución.
- **Remote Services: SMB/Windows Admin Shares:** Los adversarios pueden usar cuentas válidas para interactuar con un recurso compartido de red remoto mediante el bloque de mensajes del servidor (SMB). El adversario puede entonces realizar acciones como el usuario que inició sesión. Los adversarios pueden usar SMB para interactuar con archivos compartidos, lo que les permite moverse lateralmente a través de una red.

CVSS:

SMB/Windows Admin Shares:

Base Score

7.7
(High)

Attack Vector (AV)	Scope (S)
<input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)	<input type="radio"/> Unchanged (U) <input checked="" type="radio"/> Changed (C)
Attack Complexity (AC)	Confidentiality (C)
<input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)
Privileges Required (PR)	Integrity (I)
<input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)
User Interaction (UI)	Availability (A)
<input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)	<input checked="" type="radio"/> None (N) <input type="radio"/> Low (L) <input type="radio"/> High (H)

Los recursos compartidos de red incluyen C \$, ADMIN \$ e IPC \$. Los adversarios pueden utilizar esta técnica junto con cuentas válidas de nivel de administrador para acceder de forma remota a un sistema en red a través de SMB, para interactuar con sistemas mediante llamadas a procedimientos remotos (RPC)

Create or Modify System Process: Windows Service

Base Score

7.8
(High)

Attack Vector (AV) <div>Network (N) Adjacent (A) Local (L) Physical (P)</div>	Scope (S) <div>Unchanged (U) Changed (C)</div>
Attack Complexity (AC) <div>Low (L) High (H)</div>	Confidentiality (C) <div>None (N) Low (L) High (H)</div>
Privileges Required (PR) <div>None (N) Low (L) High (H)</div>	Integrity (I) <div>None (N) Low (L) High (H)</div>
User Interaction (UI) <div>None (N) Required (R)</div>	Availability (A) <div>None (N) Low (L) High (H)</div>

Los adversarios pueden crear o modificar servicios de Windows para ejecutar repetidamente payloads. Los servicios pueden crearse con privilegios de administrador, pero se ejecutan bajo privilegios de SISTEMA, por lo que un adversario también puede usar un servicio para escalar privilegios de administrador a SISTEMA. Los adversarios también pueden iniciar servicios directamente a través de la ejecución del servicio.

Hijack Execution Flow: COR_PROFILER

Base Score

7.8
(High)

Attack Vector (AV) <div>Network (N) Adjacent (A) Local (L) Physical (P)</div>	Scope (S) <div>Unchanged (U) Changed (C)</div>
Attack Complexity (AC) <div>Low (L) High (H)</div>	Confidentiality (C) <div>None (N) Low (L) High (H)</div>
Privileges Required (PR) <div>None (N) Low (L) High (H)</div>	Integrity (I) <div>None (N) Low (L) High (H)</div>
User Interaction (UI) <div>None (N) Required (R)</div>	Availability (A) <div>None (N) Low (L) High (H)</div>

Los adversarios pueden abusar de COR_PROFILER para ejecutar una DLL maliciosa en el contexto de todos los procesos .NET cada vez que se invoca CLR. El COR_PROFILER también se puede utilizar para elevar privilegios o por ejemplo omitir el control de acceso del usuario.

Web Service: Bidireccional Comunicación

Base Score

3.1
(Low)

Attack Vector (AV) <div>Network (N) Adjacent (A) Local (L) Physical (P)</div>	Scope (S) <div>Unchanged (U) Changed (C)</div>
Attack Complexity (AC) <div>Low (L) High (H)</div>	Confidentiality (C) <div>None (N) Low (L) High (H)</div>
Privileges Required (PR) <div>None (N) Low (L) High (H)</div>	Integrity (I) <div>None (N) Low (L) High (H)</div>
User Interaction (UI) <div>None (N) Required (R)</div>	Availability (A) <div>None (N) Low (L) High (H)</div>

El tráfico de retorno puede producirse de diversas formas, según el servicio web que se utilice. Por ejemplo, el tráfico de retorno puede tomar la forma de un sistema comprometido que publica un comentario en un foro, envía una solicitud de extracción al proyecto de desarrollo, actualiza un documento alojado en un servicio web o envía un Tweet. Exfiltrar información principalmente.

Access Token Manipulation

Base Score

6.5
(Medium)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

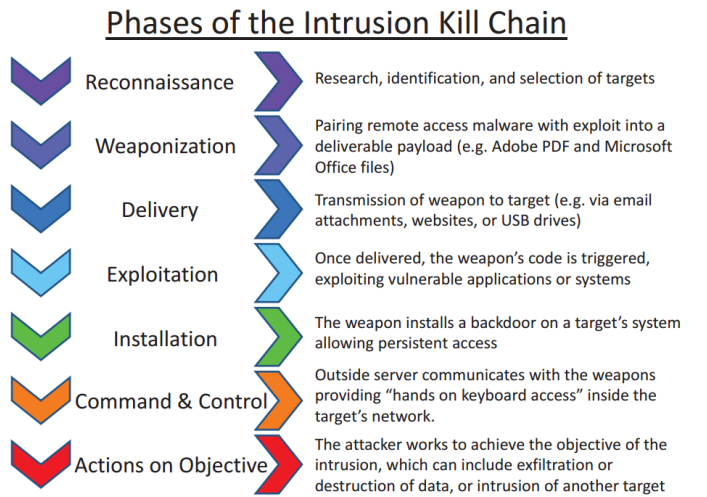
Availability (A)

None (N) Low (L) High (H)

Los adversarios pueden modificar los tokens de acceso para operar bajo un contexto de seguridad de sistema o usuario diferente para realizar acciones y evitar los controles de acceso. Windows usa tokens de acceso para determinar la propiedad de un proceso en ejecución.

2. Cyber Kill Chain

Este concepto divide los ataques cibernéticos en un total de siete niveles, que un perpetrador debe alcanzar sucesivamente para poder implementar su plan. Por el contrario, a nivel de defensa es posible bloquear todo el ataque del cibercriminal interrumpiéndolo en un nivel. Sin embargo, es aconsejable construir una defensa de varios niveles, ya que de lo contrario el atacante podría atacar de nuevo a través de uno de los niveles anteriores.



1. **Reconocimiento:** el intruso selecciona el objetivo, lo investiga e intenta identificar vulnerabilidades en la red objetivo.
2. **Armamento:** Intruso crea un arma de malware de acceso remoto, como un virus o un gusano, adaptada a una o más vulnerabilidades.
3. **Entrega:** el intruso transmite el arma al objetivo (por ejemplo, a través de archivos adjuntos de correo electrónico, sitios web o unidades USB)
4. **Explotación:** se activa el código del programa del arma de malware, que toma medidas en la red de destino para aprovechar la vulnerabilidad.
5. **Instalación:** el arma de malware instala un punto de acceso (por ejemplo, "puerta trasera") que puede utilizar el intruso.
6. **Comando y control:** el malware permite que el intruso tenga acceso persistente "con las manos en el teclado" a la red de destino.
7. **Acciones sobre el objetivo:** el intruso toma medidas para lograr sus objetivos, como la exfiltración de datos, la destrucción de datos o el cifrado para obtener un rescate.

Basándose en estas etapas de Cyber Kill Chain, se toma la perspectiva del atacante. En términos concretos, esto significa que para cada nivel individual el atacante tiene que considerar qué herramientas o posibilidades tiene para implementar su plan.

3. Multas a una organización por incumplimiento

Ley GDPR/ ISO27001

La compañía **alemana Knuddels**, una empresa alemana de mensajería ha sido sancionada con el pago de 20.000 euros por filtrar más de 808.000 direcciones de correo electrónico y más de 1,8 millones de nombres de usuario y contraseñas. En julio de este año, la plataforma de chat de Knuddels sufrió una violación de datos y la información robada de sus servidores se publicó en línea de forma transparente. Este incidente demuestra que es imperativo integrar soluciones de encriptación de datos que eviten las filtraciones de información sensible de carácter personal.

Ley HIPAA

Touchstone Medical Imaging fue multado con 3.000.000 USD por exponer una carpeta de forma pública en un servidor ftp con información de 307.839 pacientes.

En mayo de 2014, la Oficina Federal de Investigaciones (FBI) y la OCR notificaron a Touchstone que uno de sus servidores FTP permitía el acceso incontrolado a la información médica protegida (PHI) de sus pacientes. Este acceso incontrolado permitió a los motores de búsqueda indexar la PHI de los pacientes de Touchstone, que permaneció visible en Internet incluso después de desconectar el servidor.

Practica 1 – TEMA 4

1. Cifrar con OpenSSL

Vamos a cifrar con OpenSSL en nuestra maquina Kali ya que en Windows es igual pero más difícil de instalar

Creamos un archivo llamado **secreto.txt** que contiene “hola” y la ciframos con **AES-128**

```
lecikt@kali:~$ openssl enc -aes-128-cbc -a -in secreto.txt -out aes_cbc.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
lecikt@kali:~$ cat aes_cbc.txt
U2FsdGVkX1+xmswn1HGwrcIxMEAF/Ifkn84P82Q2VRIXZ1DJ2nRGMQQ3efJYKRvz
lecikt@kali:~$
```

A continuación, ciframos el mismo fichero con **DES**

```
lecikt@kali:~$ openssl enc -des-ecb -a -in secreto.txt -out des_ecb.txt
enter des-ecb encryption password:
Verifying - enter des-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
lecikt@kali:~$ ls
Descargas  des_ecb.txt  Documentos  Escritorio  Imágenes  Música  Plantillas  prod.dtsC
lecikt@kali:~$ cat des_ecb.txt
U2FsdGVkX1/x8wrjCDcxXREawVuDIg3sqYcSXP4dYoA+dsecR/20Gw==
lecikt@kali:~$
```

HastCat por otro lado si lo vamos a usar en Windows debido a que en mi Kali no tiene los archivos diccionario o no los encuentra

```
lecikt@kali:~$ hashcat -a 3 -m 14000 U2FsdGVkX1/x8wrjCDcxXREawVuDIg3sqYcSXP4dYoA+dsecR/20Gw==
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform
=====
* Device #1: pthread-Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz, 5636/5700 MB (2048 MB allocatable), 1M

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 8

Hash 'U2FsdGVkX1/x8wrjCDcxXREawVuDIg3sqYcSXP4dYoA+dsecR/20Gw==': Separator unmatched
No hashes loaded.

Started: Sat Oct 24 12:50:39 2020
Stopped: Sat Oct 24 12:50:39 2020
lecikt@kali:~$ hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
hashcat (v6.1.1) starting...

example.dict: No such file or directory

Started: Sat Oct 24 12:54:49 2020
Stopped: Sat Oct 24 12:54:49 2020
lecikt@kali:~$
```

Una vez descargado y funcionando en Windows vemos que si tiene los archivos diccionario

```
C:\Users\ramon\Documents\Universidad 2021\Primer Q\Introduccion a la seguridad informatica\hashcat-6.1.1>hashcat.exe -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
hashcat (v6.1.1) starting...
```

Nos muestra los hashes descifrados

Approaching final keyspace - workload adjusted.

```
e11c594e6a2f4eb499cceedfca988595:13LEXON
dcca2ed1630582435afa9d42ce361eb4:Admin11
ff271392937d28d7eff2d0faefdb92cf:andzia123
d620cb449339aada319d5905e66d7924:azerty130
0426b809c0ee71d48407bc86461688d9:brain01
7bf7234ba9620f43cf43c87c13e9a4f6:c0nc0rd1
146dc5ff7a16eebf5b9af81162706e0a:casimir13
81879b7503aaf122211385e9d977fa08:casillas23
f4719a14434de8f027ceb7d31fe9f6fb:christophe69
187655e4c9aff47ec2888f0cc2942efe:daniel179
a08c354f925b2a9df839290c8903c1e9:dodge15
a0bd161255f5f0c74ad6aa04e68b06a2:eyal123
0a3edab1955f9bf2cf6f8a808456b89b:findus123
86d3bc5436335ce3be44f4b8520c4506:francisca01
1dca20e382b4b72e4d8ae172eb3dd2c6:gustave01
```

No puedo sacar la contraseña con hashcat porque no entiendo cómo funciona enseñare los ejemplos de cómo debería hacerse, pero con mis archivos no soy capaz, incluso he probado con CyberChef y tampoco soy capaz de descifrarlo, lo muestro a continuación.

Esta es mi contraseña que he cifrado con Base64 y con DES en cyberchef:

Recipe	Input
<p>From Base64</p> <p>Alphabet A-Za-z0-9+/=</p> <p><input checked="" type="checkbox"/> Remove non-alphabet chars</p>	<p>U2FsdGVkX1/x8wrjCDcxXREawVuDIg3sqYcSXP4dYoA+dsecR/20Gw==</p> <p>Output</p> <p>Salted__ñó ã.71]..Ã[." i0...\p.b.>vÇ.Gý..</p>

Y luego supuestamente esto ya es DES

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

DES Decrypt

Key

UTF8

IV

BASE64

Mode

ECB

Input

Raw

Output

Hex

Input

U2FsdGVkX1/x8wrjCDcxXREawVuDIg3sqYcSXP4dYoA+dsecR/20Gw==

Output

Invalid key length: 0 bytes

DES uses a key length of 8 bytes (64 bits).
Triple DES uses a key length of 24 bytes (192 bits).

Y nos da este error.

Como habría que hacer el ataque de fuerza bruta con Hascat:

Estos son los ejemplos que proporciona hashcat, vemos la línea de Fuerza bruta

Attack-Mode	Hash-Type	Example command
Wordlist	\$P\$	hashcat -a 0 -m 400 example400.hash example.dict
Wordlist + Rules	MD5	hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
Brute-Force	MD5	hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a
Combinator	MD5	hashcat -a 1 -m 0 example0.hash example.dict example.dict

-a para especificar el tipo de ataque (3 = Fuerza bruta)

-m para cargar el tipo de Hash (14000 en mi caso porque es DES)

Los tipos de char-sets que vienen incorporados:

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?s = !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
- ?a = ?l?u?d?s
- ?b = 0x00 - 0xff

Pero no entiendo como pasar mi clave para que hashcat la analice y la rompa en el caso del cifrado DES.

En el caso de AES ni lo intento AES256 sería una locura con fuerza bruta. Si tuviera 2.000 petaFLOPS (la supercomputadora más rápida de la actualidad tiene unos 93 petaFLOPS), se necesitarían 67.000.000.000.000.000.000.000.000.000.000 años para agotar el espacio clave de AES256. El universo solo ha tenido alrededor de 14,000,000,000 de años, para dar una sensación de escala.

2. Criptoanálisis para algoritmos simétricos

Tendencias actuales en el criptoanálisis

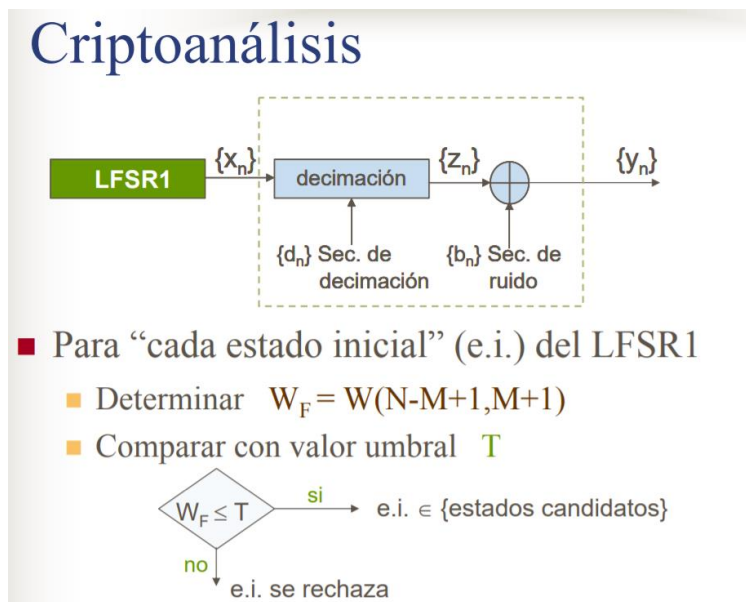
- Técnica de la “edit distance”
- Slide attack
- Ataques sobre implementación de software

Edit distance:

El menor número de operaciones elementales de edición requeridas para transformar la secuencia X en la secuencia Y (Distancia de Levenshtein, 1966)

Cifrado en flujo (Secuencias de distinta longitud)

La forma de ataque es determinar el estado inicial de los registros de desplazamiento LFSRs que intervienen en el generador



Criptoanálisis sobre Advanced Encryption Standard (AES) a través de medidas de radiación electromagnética:

Una de las técnicas de criptoanálisis más utilizada es el análisis por Side Channel (SCA por sus siglas en inglés). La técnica se basa en monitorizar el consumo de potencia o la radiación electromagnética de un dispositivo durante la ejecución de un algoritmo criptográfico. El objetivo es el de, mediante observación y análisis estadístico de las operaciones monitorizadas, llegar a extraer datos confidenciales del algoritmo como su clave secreta.

Blowfish

El algoritmo es considerado seguro aunque se han descubierto algunas claves débiles, un ataque contra una versión del algoritmo con tres rotaciones y un ataque diferencial contra una variante del algoritmo.

3. 'Salt' en un algoritmo simétrico

Comprende bits aleatorios que se usan como una de las entradas en una función derivadora de claves. La otra entrada es habitualmente una contraseña. La salida de la función derivadora de claves se almacena como la versión cifrada de la contraseña. La sal también puede usarse como parte de una clave en un cifrado u otro algoritmo criptográfico. La función de derivación de claves generalmente usa una función hash. A veces se usa como sal el vector de inicialización, un valor generado previamente.

¿Porque aporta más seguridad al cifrado? Pues porque las sales también hacen mucho más lentos los ataques de diccionario y los ataques de fuerza bruta al crackear grandes cantidades de contraseñas (pero no en el caso de crackear sólo una contraseña). Sin las sales, un atacante que está crackeando muchas contraseñas al mismo tiempo sólo necesita generar un hash y compararlo con los demás hashes. En cambio, con sales, todas las contraseñas tendrán diferentes sales, por lo que cada intento deberá ser hasheado por separado para cada sal, lo que es mucho más lento debido a que la generación de hashes usualmente consume muchos recursos computacionales.

Ejemplo:



Say the password I want to salt looks like this:

```
7X57CKG72JVNSSS9
```

Your salt is just the word SALT

Before hashing, you add SALT to the end of the data. So, it would look like this:

```
7X57CKG72JVNSSS9SALT
```

El valor hash es diferente de lo que sería solo para la contraseña simple sin sal. Incluso la más mínima variación de los datos que se procesan dará como resultado un valor hash único diferente. Al saltar su contraseña, esencialmente está ocultando su valor hash real agregando un poco de datos adicionales y modificándolos.

Ahora, si un atacante de fuerza bruta conoce tu sal, es esencialmente inútil. Pueden simplemente agregarlo al final de cada variación de contraseña que estén intentando y eventualmente encontrarlo. Es por eso por lo que la sal para cada contraseña debe ser diferente: para protegerse contra los ataques de rainbow table.

4. Principales técnicas de esteganografía hoy día

- **Esteganografía en tecnologías web:** Aprovechar la propia arquitectura del lenguaje de maquetado para ofuscar información. Como bien sabe, HTML no distingue entre mayúsculas y minúsculas, por lo que para el navegador
 sería lo mismo que
, que
 o que
. Y ahí tenemos varias alternativas distintas que funcionan de la misma manera.

(Ocultan información basada en mensajes simples)

- **Esteganografía hardware:** La estructura final de los datos almacenados en un medio físico también puede facilitar la creación de mecanismos de ocultación de información, ya sea en un disquete, en un CD/DVD-ROM, un disco duro, una tarjeta flash, un chip, una tarjeta SIM, un chip de memoria (por ejemplo el que almacena la BIOS del PC)

Todas estas técnicas, pueden ser usadas para ocultar información, ya que cualquier procedimiento no estándar que se realice es habitual que pase desapercibido para el sistema operativo. Aprovechándose, precisamente de la división de un disquete en bloques lógicos llamados sectores (habitualmente de 512 bytes), la herramienta esteganografía S-tools (módulo FDD) es capaz de ocultar datos en los sectores libres de un disquete con sistema operativo DOS y sistema de ficheros FAT (File Allocation Table). Esta asignación se realiza por medio de un generador pseudoaleatorio y en ningún caso los bloques se marcan como usados.

Hoy día se pueden crear canales encubiertos o ejecución de "código de interés" (programas, malware, etc.) incluso a nivel físico de circuitos, esta situación podría ser crítica si se importan componentes electrónicos de ciertos países y estos se utilizan en infraestructuras que manejan información reservada.

- **Esteganografía en formato de ficheros:** Ofuscamos información en las limitaciones propias del fichero, o de los elementos de control de los sistemas encargados de leer el fichero. La más conocida y sencilla es la Técnica de Final de Fichero (EOF), que aprovecha el poco control a la hora de leer un fichero para ocultar información al final de este. La mayoría de los sistemas solo leen la información necesaria, por lo que se puede agregar contenido adicional que pasará desapercibido.

Hoy día, esta técnica es usada, por su sencillez y capacidad de ocultación, ampliamente para la **distribución de material protegido por derechos de autor y pornografía adulta.**

- **Esteganografía en contenido multimedia:** Tanto en imágenes como en sonido o vídeo. Las técnicas aplicadas en esteganografía de imágenes son muy parecidas a las aplicadas en sonido (basadas normalmente en ocultar información de poco peso en

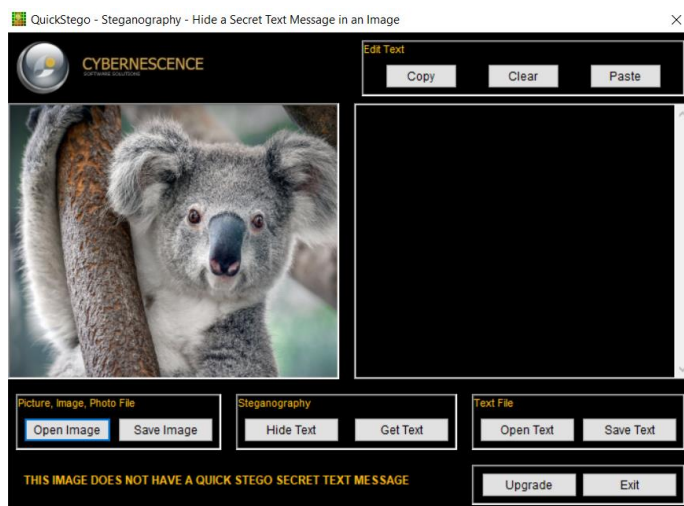
elementos muy pequeños del sistema de archivos multimedia, por ejemplo a nivel de píxeles en imágenes). En vídeo encontramos técnicas cruzadas de los dos anteriores, con algunas nuevas en las que interfiere movimientos específicos (guardar información cuando una zona cambie bruscamente de tonalidad) o en ejes críticos (subidas de volumen o espacios que cumplan x particularidad).

- Imágenes : Las técnicas y variantes más documentadas de estos procedimientos consisten en la modificación de **los LSB (Least Significant Bit)** de los píxeles de una imagen, de los índices que enlazan a la paleta de colores de un formato GIF (otros procedimientos como el reordenamiento de los colores de la paleta es posible) o de los **coeficientes resultantes de aplicar alguna transformación matemática** a una imagen.
- Audio : En los últimos años se han publicado múltiples procedimientos estenográficos y estegoanalíticos en señales de audio: técnicas basadas en **LSB (Least Significant Bit)** en muestras de audio, como la herramienta stegowav, técnicas de ocultación en la **fase de una señal** (modulación de la fase de una señal y codificación en la fase, phase coding), técnicas de ocultación en el **eco de una señal**, ocultación aprovechando las características estadísticas de las señales de audio (por ejemplo, segmentación de la señal de audio de forma adaptativa), **ocultación basada en algoritmos de compresión** (MP3, WMA, OGG Vorbis)
- Vídeo : codificación de información a partir del cálculo de los vectores de movimiento entre una colección de frames, técnicas basadas en corrección de errores

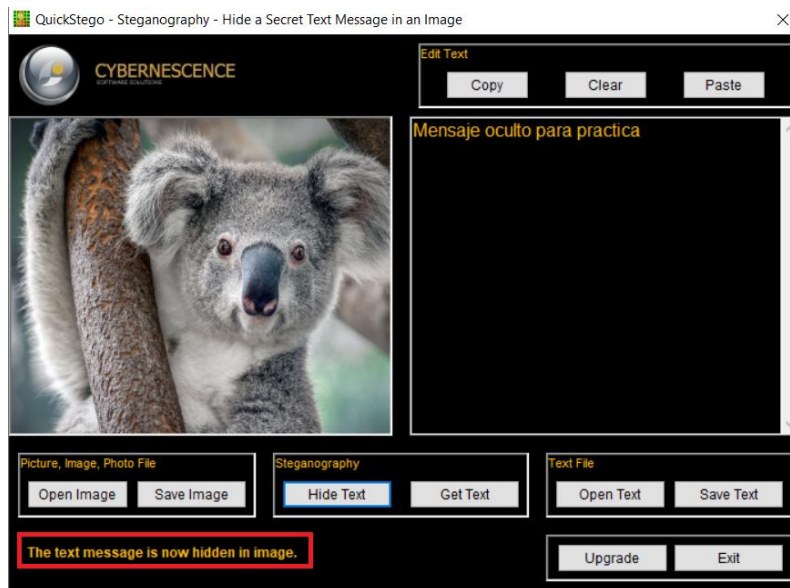
Hoy en día estas técnicas son usadas para ocultar cualquier tipo de información

Esteganografía en imágenes con QuickStego:

1. Seleccionamos la foto donde vamos a ocultar el mensaje

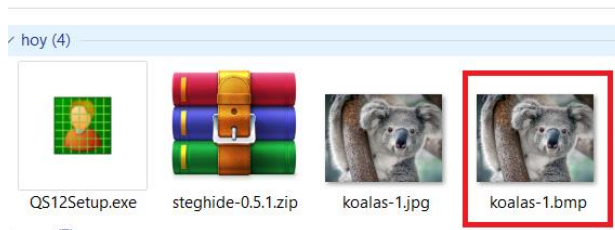


2. Escribimos el mensaje para ocultar, pulsamos en “Hide Text”



3. Guardamos nuestra imagen, esa es la imagen con el mensaje oculto

equipo > Descargas



4. Solo con abrir la imagen ya nos aparece el mensaje que contiene

