Seguridad Informática

Tema 3 – Anatomía de un ataque

Universidad Rey Juan Carlos

Antonio González Pardo **antonio.gpardo@urjc.es**

07/02/2023

Índice

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Índice

Universidad Rey Juan Carlos

- **Introducción.**
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Introducción

- Ataque es un incidente de seguridad malintencionado.
  - En el tema anterior lo definimos como “Materialización voluntaria o involuntaria de una amenaza”.

- Ataque es la materialización de una amenaza sobre una vulnerabilidad, y que provoca un daño cuantificable sobre un activo informático.

Introducción

- Los ataques se pueden catalogar como activos o pasivos, dependiendo de las acciones del atacante.
- Algunos ejemplos de ataques:
  - **Intercepción**
  - **Fabricación**
  - **Interrupción**
  - **Modificación**

Introducción

- Algunos ejemplos de ataques:
  - **Intercepción**: espionaje y/o redirección de comunicaciones para tener acceso a los que no se está autorizado (pasivo).
  - **Fabricación**: creación de un activo falso para engañar al usuario (activo).
  - **Interrupción**: bloqueo del normal funcionamiento de un activo o de una comunicación (activo).
  - **Modificación**: alteración no autorizada de un activo (activo).

Introducción

- Ejemplos de atacantes:
  - **Black Hat hackers**
    - Aprovechan las vulnerabilidades de los sistemas con diferentes objetivos. Ponen de manifiesto sus altos conocimientos y no revelan los agujeros descubiertos.
  - **White Hat hackers (hackers éticos)**
    - Atacantes que informan siempre de las vulnerabilidades descubiertas y que incluso pueden llegar a colaborar en la subsanación. Suelen ser profesionales de la “seguridad ofensiva” o expertos interesados en el avance del área.
  - **Script kiddies**
    - Atacantes aficionados sin nivel suficiente de conocimientos técnicos que utilizan herramientas automáticas y recetas cuyo funcionamiento y consecuencias desconocen.
  - **Crackers**
    - Atacantes que se centrar en romper los sistemas criptográficos.

Índice

- Introducción.
- **Técnicas de Hacking.**
- Fases de un ataque.
- Técnicas de recogida de información.
- Anonimato.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Recopilación de Información: (T3)
  - Footprinting
  - Fingerprinting:
    - Ingeniería Social, Phishing.
    - Smishing, Sniffing, Scanning…
- Ataques en red: (T4)
  - ARP Poisoning y Spoofing.
  - Man in the Middle.
  - TCP Hijacking o secuestro de sesión.
  - Ataques en la capa de aplicación.
  - Ataques a IPv6.
  - Ataques DDoS.
- Malware. (T5)
- Desbordamiento de Buffer. (T6)
- Inyecciones: (T6)
  - Inyecciones en servidor: comandos y código.
  - Inyecciones en cliente: XSS, XSRF o CSRF, etc.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Recopilación de información:
  - **Footprinting**: se centra en la recolección de información pública de Internet. Su uso no conlleva la vulnerabilidad de ninguna ley, y por lo tanto, no es delito.
  - **Fingerprinting**: consiste en recolectar información más específica y que no es pública, lo tanto es delito:
    - **Ingeniería Social**: consiste en basarse en la buena/mala fe de las personas de una organización para obtener información valiosa de ellas para realizar los ataques.
    - **Phishing**: enviar información confiable masivamente por medio del correo electrónico, en busca de información que se quiere conseguir de usuarios.
    - **Smishing**: lo mismo que el phishing pero por SMS.
    - **Sniffing**: técnica que permite capturar todos los datos que circulan por una red de área local.
    - **Scanning/Mapping**: consiste en analizar el estado de una determinada red y de los dispositivos ubicados en ella.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataques en red (Tema 4):
  - **ARP Poisoning**: consiste en envenenar las cachés ARP de las víctimas.
  - **ARP Spoofing**: ataque que consiste en enviar mensajes falsos ARP a una LAN para suplantar una identidad en la capa de enlace.
  - **Man In The Middle (MiM)**: ataque en el que se adquiere la capacidad de leer y modificar un mensaje destinado a la víctima, sin que esta sea consciente.
  - **TCP Hijacking o secuestro de sesión**: (es un tipo de MiM), el atacante consigue acceso a la conexión TCP de la víctima. El atacante puede leer y modificar los paquetes enviados y también enviar los suyos propios.
  - Ataques en la capa de aplicación:
    - **DNS Poisoning**: envenamiento de DNS.
    - **Typosquatting**: aprovechar errores tipográficos al teclear nombres de dominio.
  - **Ataques DDoS**: se intenta saturar el ancho de banda del recurso objetivo mediante el envío masivo de peticiones.

Técnicas de Hacking

Universidad Rey Juan Carlos

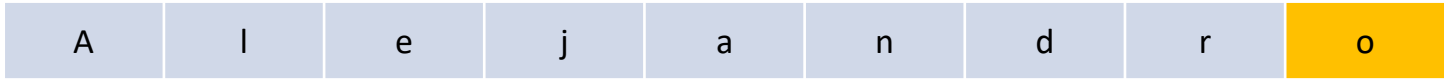
- Malware (Tema 5):
  - *Malware -> **Mal**icious Soft**ware***
  - "Malware" describe cualquier programa o código malicioso que es dañino para los sistemas.
  - Propagación:
    - Descarga, sin saberlo, del malware: accediendo al vínculo de un correo electrónico, porque viene incrustado en un torrent, o en un software de descarga gratuita.
  - Una vez instalado, el equipo está infectado y el malware empieza a trabajar para conseguir su objetivo:
    - **Ransomware**: se bloquea, y/o se deniega, el acceso al dispositivo (por medio de encriptación) y se pide un rescate.
    - **Spyware**: recaba información de la víctima como datos personales, credenciales, información financiera… etc.
    - **Adware**: el objetivo es generar ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada.

- Desbordamiento de buffer (tema 6):
  - Se genera cuando el programa no controla adecuadamente cuánta información se copia en un buffer.
  - La información que sobra se almacena en zonas de memoria adyacentes, sobre-escribiendo su contenido original.

  - Ejemplo:
    - Desarrollamos una app, que requiere un login.
    - Decidimos que el username sea un array de 8 bytes:

```
char username[8];
```


    - El usuario introduce el nombre: “Alejandro”



Técnicas de Hacking

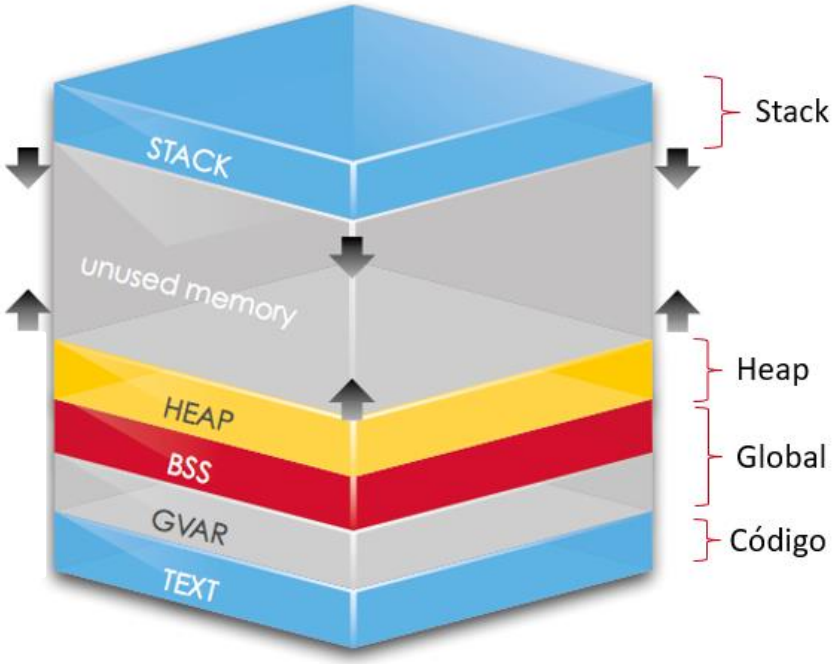
Universidad Rey Juan Carlos

- Con esta técnica podemos escribir en áreas destinadas a almacenar código ejecutable, y reemplazar el código existente por código malicioso.

- Existen lenguajes de programación que son vulnerables a esta técnica como C o C++.

- Otros lenguajes más modernos como Java, Python o C# ya contienen procedimientos para reducir las probabilidades de que se generen este tipo de ataques.

- Algo parecido se utiliza para desbordar el heap o el stack.



- No debemos olvidar el desbordamiento de los tipos básicos.

Un `int` en `Java` tiene el rango [-2147483648, 2147483647]

Técnicas de Hacking

Universidad Rey Juan Carlos

- Inyecciones en servidor:
  - **Inyección de comandos del SO (Shell injections)**: es una vulnerabilidad web que permite al atacante ejecutar comandos del sistema operativo en el servidor.
  - **Inyección SQL**: consiste en ejecutar código SQL para obtener información de la base de datos.
  - **Xpath injection**: se producen cuando un sitio web utiliza la información suministrada por el usuario para construir una consulta XPath para datos XML.

Técnicas de Hacking

- Inyecciones en cliente:
  - **XSS (Cross-site scripting)**: es un tipo de vulnerabilidad típico de las aplicaciones Web, que puede permitir a un atacante inyectar código JavaScript que se ejecutará en el navegador del cliente.
  - **XFS (Cross-frame scripting)**: el ataque explota un error específico entre marcos de scripts en un navegador web para acceder a los datos privados en un sitio web de terceros.
  - **HTTP Response Split (CRLF Injection Attack)**: es la técnica en la que un atacante se vale de la inyección de retornos de carro y saltos de línea para alterar una respuesta HTTP y separarla en dos.

Técnicas de Hacking

- Ataques de contraseñas.

- Recomendaciones para crear contraseñas:
  - No usar la misma contraseña siempre.
  - No usar datos personales
  - Usar códigos alfanuméricos.
  - Usar mayúsculas y minúsculas.
  - Utilizar símbolos.
  - Cambiar las contraseñas cada cierto tiempo.
  - Intentar definir contraseñas relativamente largas.

- Usar administrador de contraseñas.

Técnicas de Hacking

- Ataques de contraseñas: peligros
  - Decir o facilitar la contraseña a personas.
  - Apuntarlas en Post-its.
  - Ataques de Phishing.
  - Keylogger.
  - Guardar contraseñas en el navegador.
  - Publicar contraseñas.
  - Usar contraseñas habituales.
  - Ataques de fuerza bruta.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Ataque por fuerza bruta:
  - Consiste en averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.
  - El número de combinaciones de X elementos para crear una "palabra" de longitud Y es:

$$X^Y$$

Tipo de alfabeto	Longitud del alfabeto	Contraseña de longitud 5	Contraseña de longitud 10	Contraseña de longitud 15
Mayúsculas o minúsculas	26	11.881.376	$1{,}41 * 10^{14}$	$1{,}667 * 10^{21}$
Mayúsculas y minúsculas	42	130.691.232	$1{,}70 * 10^{16}$	$2{,}23 * 10^{24}$
+ números	52	380.204.032	$1{,}44 * 10^{17}$	$5{,}49 * 10^{25}$
+ símbolos	90	5.904.900.000	$3{,}48 * 10^{19}$	$2{,}05 * 10^{29}$

- Ataque por fuerza bruta:
  - Consiste en averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

- Ataques por diccionario:
  - El atacante utiliza una lista de palabras con la esperanza de que la contraseña del usuario sea una palabra de uso común o una contraseña vista en sitios anteriores.

1. 123456 (1003925)
2. 123456789 (326815)
3. 12345 (154075)
4. qwerty (143513)
5. password (106217)
6. 12345678 (103500)
7. 111111 (85937)
8. 123123 (85158)
9. 1234567890 (62649)
10. 1234567 (54441)
11. qwerty123 (51725)
12. 000000 (49286)
13. 1q2w3e (45459)
14. aa12345678 (42703)
15. abc123 (42532)
16. password1 (40939)
17. 1234 (40244)
18. qwertyuiop (38013)
19. 123321 (37380)
20. password123 (34061)

Técnicas de Hacking

Universidad Rey Juan Carlos

- Cómo funcionan las contraseñas.
- Cuando nos registramos en un servicio, nuestra contraseña no se almacena como texto en plano.

- Se almacena su resumen, o *hash*.
- Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una serie caracteres de longitud fija.

Técnicas de Hacking

Universidad Rey Juan Carlos

- “Hola”

  f688ae26e9cfa3ba6235477831d5122e

- “hola”

  4d186321c1a7f0f354b297e8914ab240

- El texto de la transparencia anterior

  51198f9794049f166e2e26cd0b8f8413

- Una captura de pantalla:

  1d7a799dd31337bd15ddfa62747ce03f

Técnicas de Hacking

- Es una función matemática, o criptográfica, que resume la información de un fichero.
- El resultado es una cadena de caracteres alfanuméricos de longitud fija, que se llama *digest*.
- Esta longitud es independiente del tamaño de la entrada.

Técnicas de Hacking

- Algunas propiedades:
  - Calcular el valor hash no conlleva mucho coste computacional.
  - Permite comprimir datos.
  - Es un proceso unidireccional: no debe ser posible obtener el valor original dado el hash.
  - No debe haber colisiones: dos entradas diferentes que generen el mismo valor hash.
- Ejemplo de funciones hash:
  - SHA
  - MD5
  - LM
  - NTLM

Técnicas de Hacking

- Las hashes son funciones irreversibles. Esto quiere decir que dado un digest, no podemos obtener la entrada que ha generado dicho resultado.
- Pero no significa que no podamos realizar ciertos tipos de ataques.
- El ataque más común consiste en pre-computar las hashes de las cadenas típicas (ataque de diccionario).
- Esto lo podemos hacer porque el cálculo de una función hash es un proceso determinista.

Técnicas de Hacking

Universidad Rey Juan Carlos

- Si conocemos la función utilizada podríamos realizar ataques de fuerza bruta sobre los hashes.
- En verdad no estamos revirtiendo el proceso de cálculo.
- Ejemplo de diccionario:

Password	MD5	SHA-1
12345	827ccb0eea8a706c4c34a16891f84e7b	8cb2237d0679ca88db6464eac60da96345513964
asdf	912ec803b2ce49e4a541068d495ab570	3da541559918a808c2402bba5012f6c60b27661c
admin	21232f297a57a5a743894a0e4a801fc3	d033e22ae348aeb5660fc2140aec35850c4da997

Técnicas de Hacking

- Existen herramientas que, dada una lista de hashes, automatizan el proceso de obtener un valor que genere dicho hash.

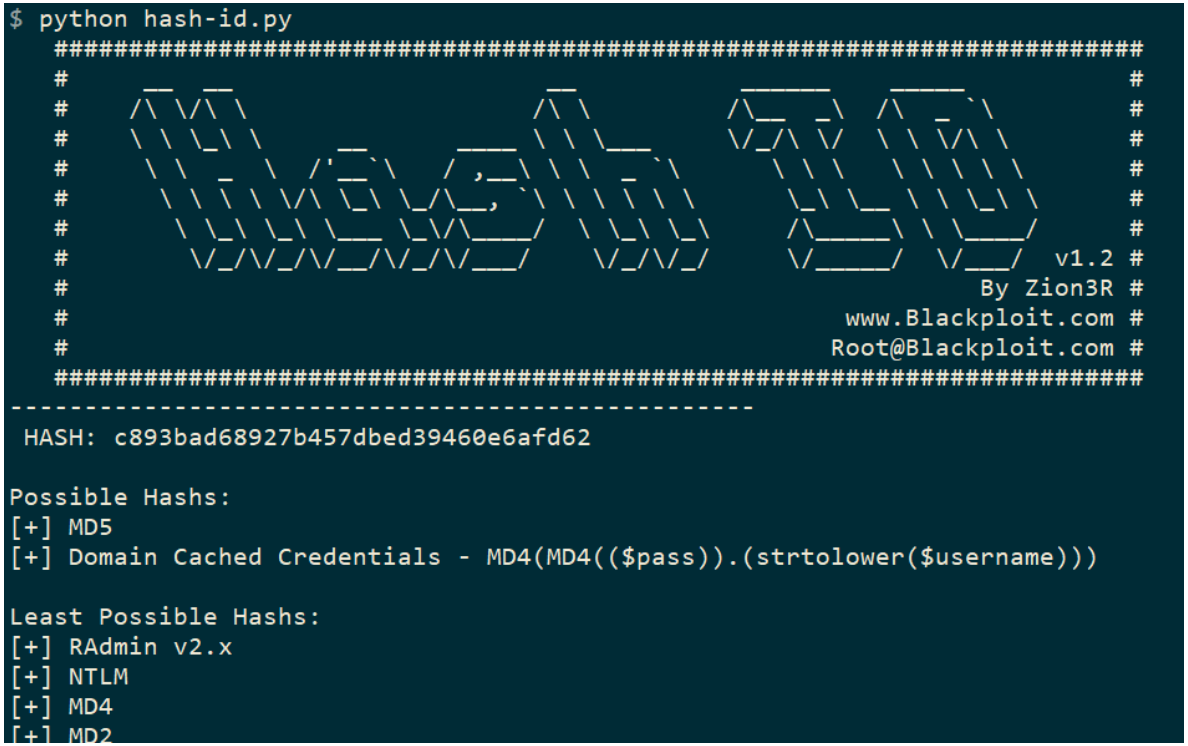
- Las más conocidas son:

Técnicas de Hacking

Universidad Rey Juan Carlos

- En muchos casos no conocemos el algoritmo hash utilizado.
- Podemos usar algunas herramientas como `hash-id`

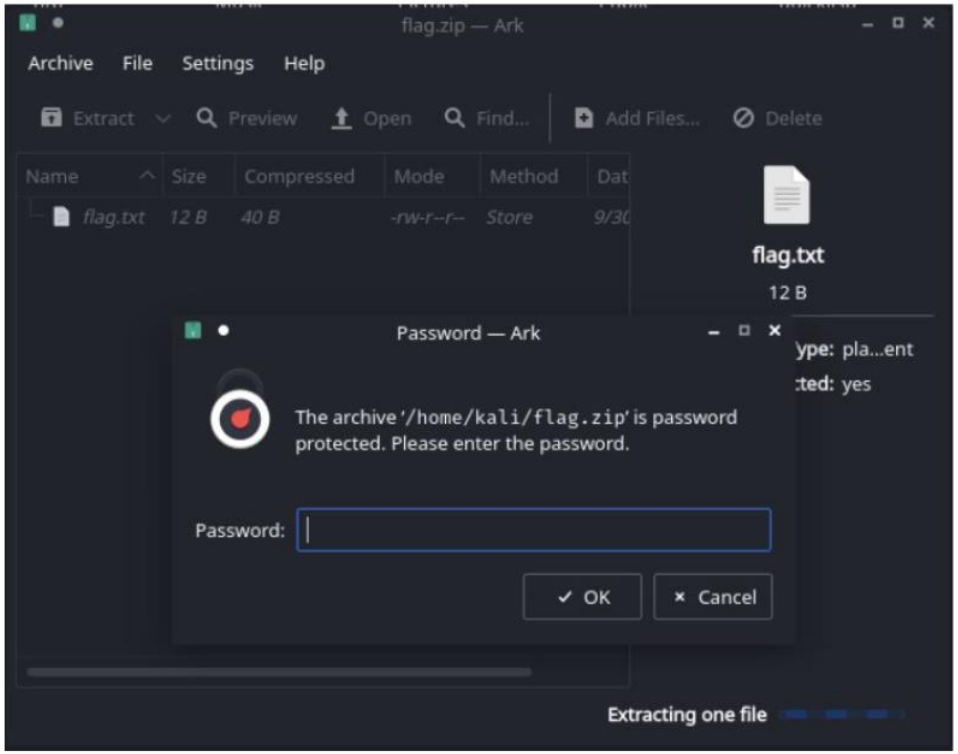
https://github.com/blackploit/hash-identifier



Caso práctico

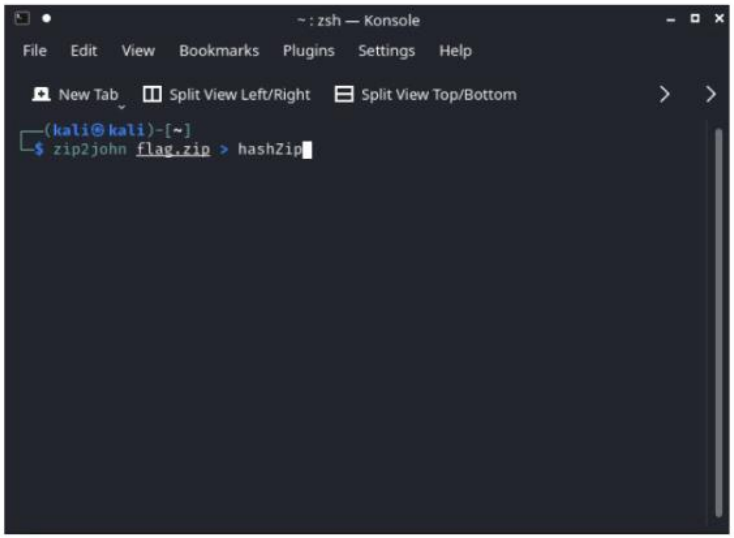
Universidad Rey Juan Carlos

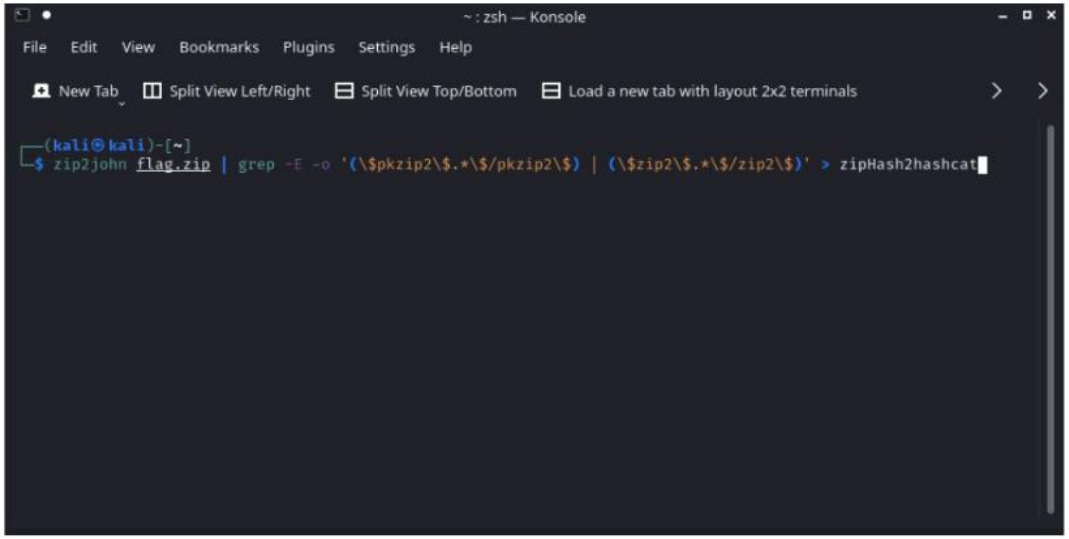
- Tanto John the Ripper como hashcat, se pueden utilizar para intentar recuperar la contraseña de un zip (por ejemplo).



Caso práctico

- PASO 1: calcular la hash del fichero





Caso práctico

- PASO 2: usar el fichero de hash con las herramientas

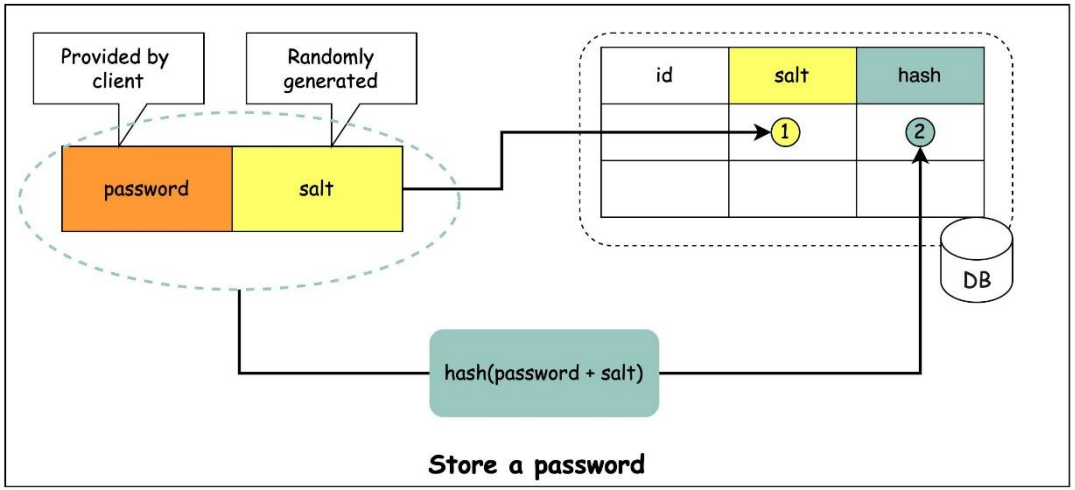

```
~ : zsh — Konsole
File  Edit  View  Bookmarks  Plugins  Settings  Help
New Tab  Split View Left/Right  Split View Top/Bottom

┌──(kali㉿kali)-[~]
└─$ john hashZip --wordlist=wordlists.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 16 needed for performance.
hola1234         (flag.zip/flag.txt)
1g 0:00:00:00 DONE (2021-09-30 16:55) 100.0g/s 100.0p/s 100.0c/s 100.0C/s hola1234
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~]
└─$ john hashZip --show
flag.zip/flag.txt:hola1234:flag.txt:flag.zip:flag.zip

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$
```

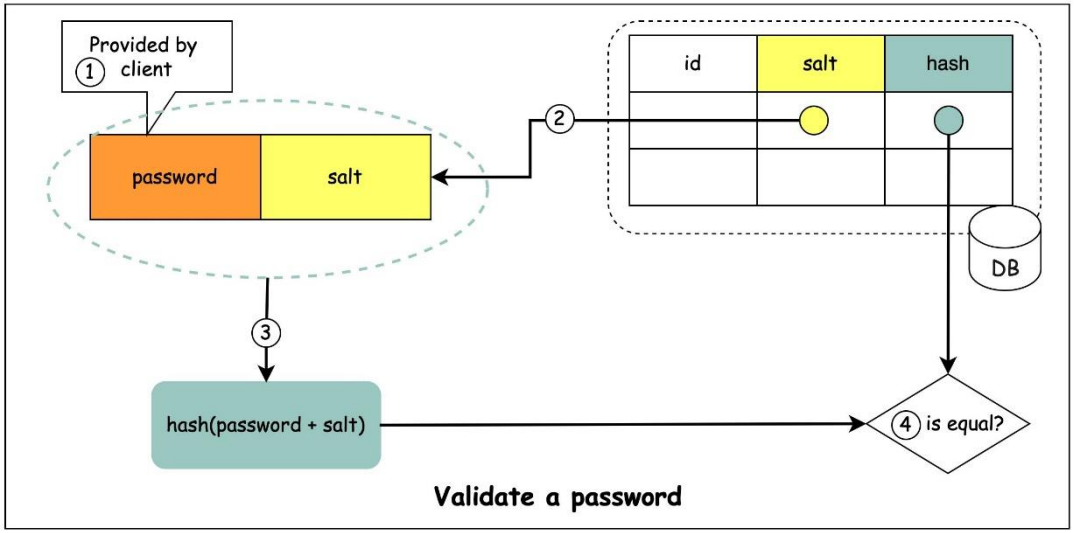
```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat ./wordlists.txt
hashcat (v6.1.1) starting ...

Session..........: hashcat
Status...........: Cracked
Hash.Name........: WinZip
Hash.Target......: $zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c* ... /zip2$
Time.Started.....: Thu Sep 30 16:59:35 2021 (0 secs)
Time.Estimated...: Thu Sep 30 16:59:35 2021 (0 secs)
Guess.Base.......: File (./wordlists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:        3 H/s (1.66ms) @ Accel:64 Loops:999 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-999
Candidates.#1....: hola1234 → hola1234

Started: Thu Sep 30 16:58:55 2021
Stopped: Thu Sep 30 16:59:37 2021

┌──(kali㉿kali)-[~]
└─$ hashcat -m 13600 zipHash2hashcat --show
$zip2$*0*3*0*f819c01513f1f5018f4e73128d711b52*8d6c*c*327662bd488eec34fe3ad3fa*4b36073395bdba927dda*$/zip2$:hola1234

┌──(kali㉿kali)-[~]
└─$
```

https://github.com/danielmiessler/SecLists

How to store passwords in DB?

blog.bytebytego.com





Ataque a la empresa hotelera IHG (InterContinental Hotels Group).
200.000 empleados tenían acceso al usuario y contraseña de la bóveda.
Noticia publicada el 20/09/2022

Índice

- Introducción.
- Técnicas de Hacking.
- **Fases de un ataque.**
- Técnicas de recogida de información.
- Anonimato.

Fases de un ataque

Universidad Rey Juan Carlos

- Un ataque no se produce sin una planificación.
- Todo ataque sigue unas fases que están bien definidas.
- Veremos las diferentes fases según 4 grandes instituciones:
  - SANS Technology Institute
  - Lookhead Martin
  - National Cyber Security Center
  - Infosec Institute.

Fases de un ataque

Universidad Rey Juan Carlos

- SANS Technology Institute:
  1. **Reconocimiento**: probar sistemas y redes para ver qué hay.
  2. **Enumeración**: recogida de información más específica del objetivo.
  3. **Brecha**: el atacante consigue penetrar en el sistema o red.
  4. **Administración**: se logra el control y acceso del sistema.
  5. **Limpieza**: se eliminan las evidencias del ataque.

Fases de un ataque

Universidad Rey Juan Carlos

- Lookhead Martin: definió 7 fases.
- Este modelo, o esta definición, ha sido globalmente aceptado.
  1. **Reconocimiento**: aprender sobre el objetivo.
  2. **Armamento**: adecuación del código malicioso o malware al medio sobre el que se busca realizar el ataque.
  3. **Entrega**: transmitir el malware.
  4. **Explotación**: aprovechar alguna vulnerabilidad en el software o error humano para ejecutar el código.
  5. **Instalación**: el malware se asegura de poder ejecutarse de forma permanente en el equipo infectado.
  6. **Comando** y **Control**: el malware se comunica con su central, proporcionando a los atacantes el control remoto.
  7. **Acciones sobre los objetivos**: se procede al robo o a la ejecución de los que se plantea hacer.

Fases de un ataque

Universidad Rey Juan Carlos

- National Cyber Security Center, UK.
  1. **Encuesta (Survey)**: investigar y analizar la información disponible sobre el objetivo para identificar vulnerabilidades.
  2. **Entrega (Delivery)**: llegar al punto en un sistema, en el que se puede explotar una vulnerabilidad.
  3. **Infracción (Breach)**: explotar la vulnerabilidad.
  4. **Efecto (Affect)**: llevar a cabo actividades dentro del sistema.

Fases de un ataque

Universidad Rey Juan Carlos

- Infosec Institute:
  1. **Reconocimiento**: identificar al objetivo.
  2. **Escaneo**: identificar el punto débil.
  3. **Acceso y escalamiento**: objetivo es entrar en el sistema y escalar privilegios o propagarse por la red.
  4. **Exfiltración**: extraer toda la información posible del sistema.
  5. **Sostenibilidad**: intentar mantenerse dentro del sistema el mayor tiempo posible.
  6. **Asalto**: alterar el funcionamiento del sistema o deshabilitar ciertas partes (hw como sw).
  7. **Ofuscación**: ocultar el rastro.

Fases de un ataque

Universidad Rey Juan Carlos

- De una manera general se necesitan las siguientes fases:
  1. **Reconocer**: recoger información.
  2. **Escanear**: probar activamente vulnerabilidades.
  3. **Obtener acceso**: explotar una vulnerabilidad.
  4. **Mantener acceso**: seguir dentro del sistema hasta alcanzar el objetivo.
  5. **Ocultación del rastro**.

Índice

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- **Técnicas de recogida de información**.
  - **Footprinting.**
  - Fingerprinting.
- Anonimato.

Footprinting

- Este proceso se centra en la recogida de información pública disponible en internet.
- Su uso no conlleva la vulneración de ninguna ley, y no es delito.
- Es la búsqueda y recolección de toda la información posible de un objetivo publicada:
  - con conocimiento, permiso o en medios públicos: Redes Sociales, blogs, prensa, BOE, boletines de las comunidades autónomas u organismos oficiales.
  - sin conocimiento: metadatos añadidos automáticamente a los archivos.

Footprinting – OSINT

Universidad Rey Juan Carlos

- La recolección de datos por medio de fuentes abiertas se conoce como OSINT (*Open Source Intelligence*)
- Inteligencia de fuentes abiertas conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información.
  - Medios de comunicación: revistas, periódicos, radio, etc.
  - Información pública de fuentes gubernamentales.
  - Foros, redes sociales, blogs, wikis, etc.
  - Conferencias, simposios, artículos, bibliotecas online, etc.
- Necesita un análisis posterior que incluye procesado de los datos.
- Problema: demasiada información y dudosa fiabilidad.

Footprinting – OSINT

Universidad Rey Juan Carlos

Fases del sistema de obtención de información:

1. **Requisitos**: se establecen todos los aquellas condiciones que deben satisfacerse para conseguir el objetivo, o resolver el problema que ha originado el desarrollo del sistema OSINT.

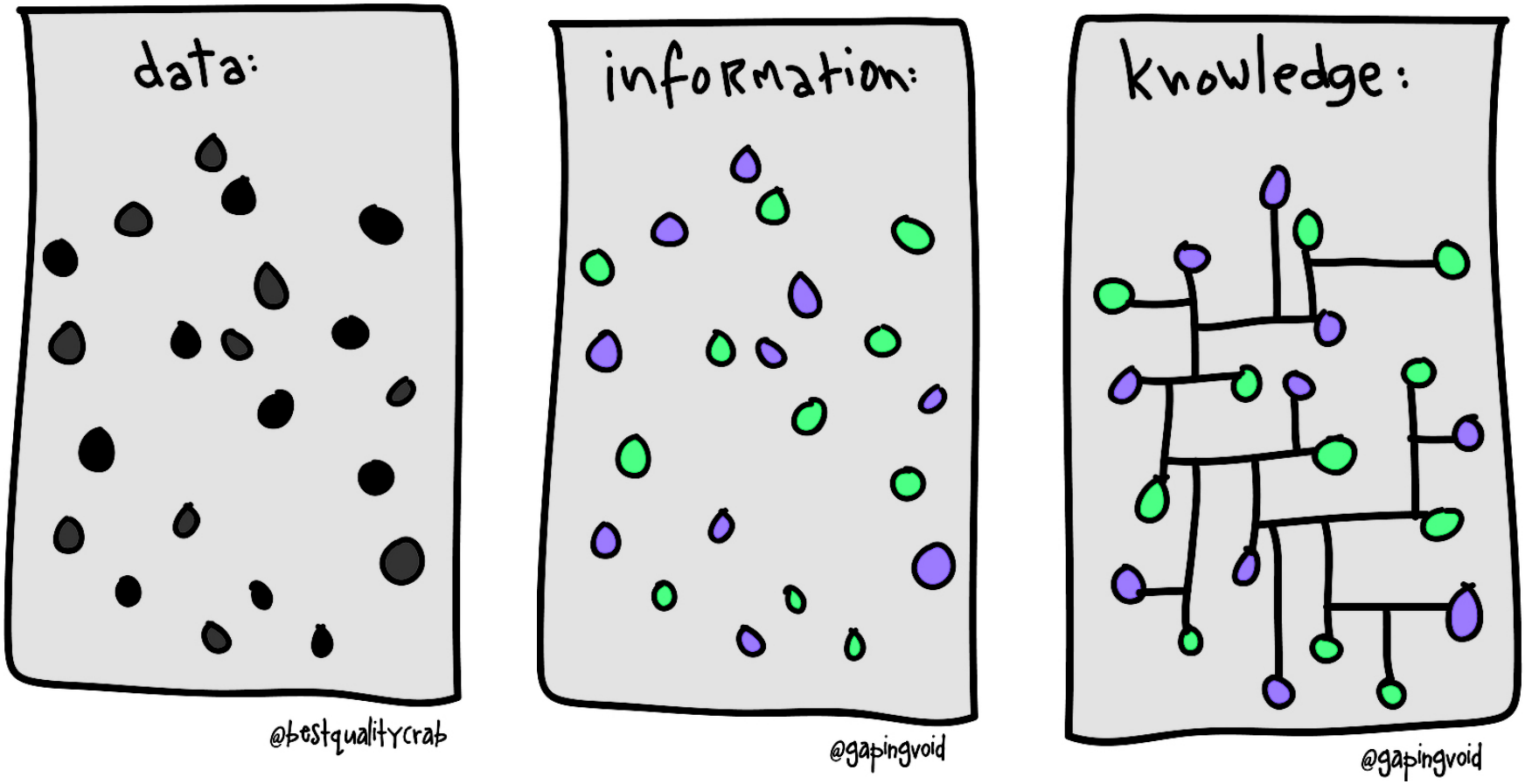
2. **Identificar fuentes de información relevante**: consiste en especificar las fuentes de interés que serán recopiladas. Se deben identificar y concretar las fuentes de información para optimizar el proceso de adquisición de datos.

Fases del sistema de obtención de información:

3. **Adquisición**: etapa en la que se obtienen los datos a partir de los orígenes indicados.
4. **Procesamiento**: consiste en dar formato a todos los datos recopilados.
5. **Análisis**: se genera inteligencia (conocimiento) a partir de los datos recopilados y procesados. El objetivo es relacionar los datos de distintos orígenes buscando patrones que permitan llegar a alguna conclusión.
6. **Presentación de inteligencia**: consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser explotada.

Footprinting – OSINT

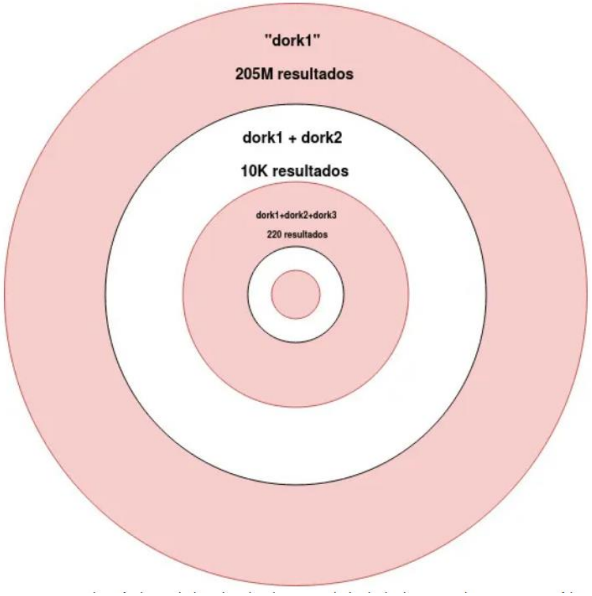
Universidad Rey Juan Carlos



Footprinting – OSINT

Universidad Rey Juan Carlos

- Una manera de extraer información es usando los “dorks”
- Es una búsqueda avanzada en buscadores aplicando filtros en la propia búsqueda.
- Aplicando diferentes dorks podremos ir afinando los resultados.



Footprinting – OSINT

Universidad Rey Juan Carlos

- Ejemplos de dorks que podemos usar:
  - “” : coincidencia exacta.
  - `site`: para buscar en un sitio web específico.
  - `filetype`, `ext`: buscar archivos que tienen una extensión determinada.
  - `intext`: buscar páginas cuyo texto contenga el parámetro
  - `intitle`: resultados con páginas en cuyo título aparece la palabra específica.
  - `OR`: operador lógico.
  - `AND`: operador lógico.
  - `-` : símbolo de exclusión.
  - `cache`: para forzar resultados que estén en la cache del sistema de búsqueda.

Footprinting – OSINT

Universidad Rey Juan Carlos

- En internet existen una gran cantidad de recursos para hacer este tipo de análisis.
- Podemos buscar usuarios en redes sociales:

  https://www.namecheckr.com/

- También podemos buscar dominios:

  https://namechk.com/

- O también podemos usar algún software específico:

  https://github.com/sherlock-project/sherlock

Footprinting – OSINT

Universidad Rey Juan Carlos

- Podría ser que busquemos información y dicha información no esté activa (o el dominio no esté activo).

- Tenemos alternativas:

https://archive.org/

- También tenemos la cache de Google:

Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT

- IMINT proviene de *IMage INTelligence.*

Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT
- IMINT proviene de *IMage INTelligence.*
- Para ese análisis podemos usar buscadores como:
  - TinEye: https://tineye.com/
  - Yandex: https://yandex.com/
  - Google Lens.
  - El buscador de fotos de Google.

Footprinting

Universidad Rey Juan Carlos

- Tenemos además otras fuentes de información:
  - IMINT
  - HUMINT
- HUMINT proviene de *HUMan INTelligence.*
- En este caso tenemos un dato personal: nombre completo, un email, número de teléfono… etc.

https://haveibeenpwned.com/

Footprinting – Metadatos

Universidad Rey Juan Carlos

- Los metadatos son aquellos datos que hablan de los datos.
- Describen el contenido de los archivos o la información de los mismos.
- Este tipo de ataques pertenecen a footprinting siempre y cuando los archivos a analizar sean públicamente accesibles.
- Los metadatos recogen información acerca de:
  - La fecha de creación y de la última modificación.
  - Los autores que han participado en la creación del archivo.
  - La aplicación empleada.
  - A veces contiene información sobre el SO, versiones, etc.
  - Se puede encontrar información de la geolocalización…etc.

Footprinting – Metadatos

Universidad Rey Juan Carlos

Cámara

Fabricante de cámara	SONY
Modelo de cámara	HDR-AS200V
Punto F	f/2.8
Tiempo de exposición	1/125 s
Velocidad ISO	
Compensación de exposición	0 paso
Distancia focal	3 mm
Apertura máxima	2.96875
Modo de medición	Diseño
Distancia al objeto	
Modo de flash	Sin función de flash
Intensidad de flash	
Longitud focal de 35 mm	

Origen

Autores	Antonio
Guardado por	Antonio Gonzalez
Número de revisión	277
Número de versión	
Nombre del programa	Microsoft Office PowerPoint
Organización	
Administrador	
Contenido creado	21/02/2021 17:10
Guardado el	23/02/2021 15:12
Fecha de impresión	
Tiempo de edición	123:01:00

Contenido

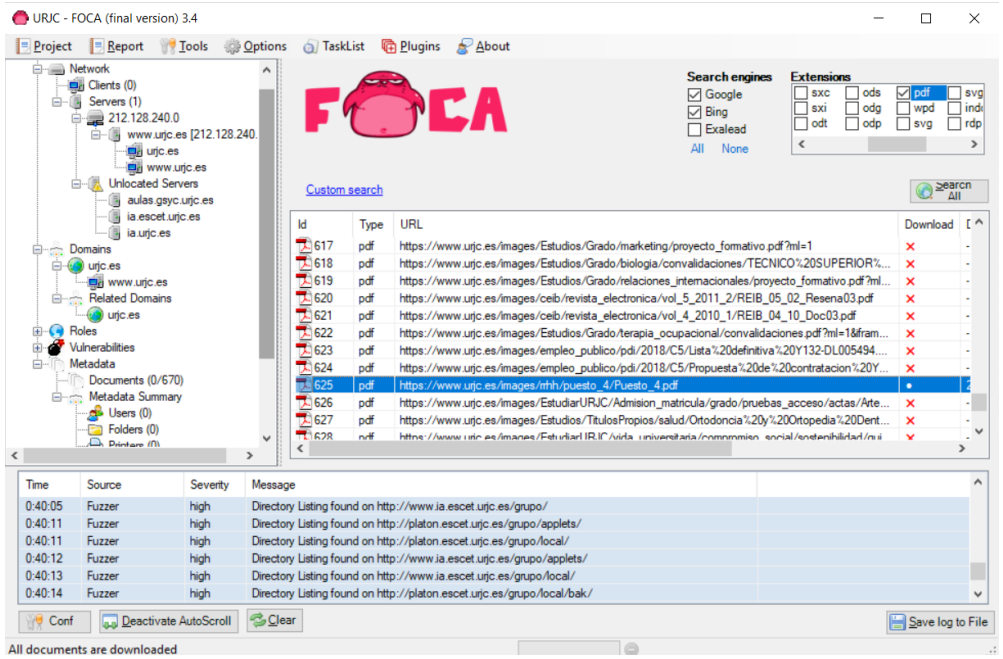
Estado de contenido	
Tipo de contenido	application/vnd.openxmlformats-...
Contar palabras	4182
Número de líneas	
Número de párrafos	636
Diapositivas	76
Notas	6
Ocultar cuenta	4
Clips multimedia	0
Formato de presentación	Presentación en pantalla (4:3)
Plantilla	
Escala	No
Vínculos obsoletos	No
Idioma	

Footprinting – Metadatos

Universidad Rey Juan Carlos

FOCA desarrollado por la compañía *elevenpaths*

- Herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina.
- Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.



Footprinting – Metadatos

Universidad Rey Juan Carlos

FOCA desarrollado por la compañía *elevenpaths*

- Herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina.
- Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Exiftool: https://exiftool.org/

```
ExifTool Version Number         : 12.40
File Name                       : Tema3 - AnatomiaAtaque.pptx
Directory                       : .
File Size                       : 5.1 MiB
File Modification Date/Time     : 2022:02:14 20:46:34+01:00
File Access Date/Time           : 2022:02:14 20:50:31+01:00
File Creation Date/Time         : 2022:02:14 20:50:29+01:00
File Permissions                : -rw-rw-rw-
File Type                       : PPTX
File Type Extension             : pptx
MIME Type                       : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x00360bc6
Zip Compressed Size             : 1228
Zip Uncompressed Size           : 6830
Zip File Name                   : ppt/presentation.xml
Title                           : Tema 3
Creator                         : Antonio Gonzalez
Last Modified By                : Antonio Gonz├ilez Pardo
Revision Number                 : 67
Create Date                     : 2021:02:24 08:08:17Z
Modify Date                     : 2022:02:14 19:46:34Z
Template                        : Clases
Total Edit Time                 : 1.8 days
Words                           : 6126
Application                     : Microsoft Office PowerPoint
Presentation Format             : Presentaci├│n en pantalla (4:3)
Paragraphs                      : 1074
Slides                          : 106
Notes                           : 12
Hidden Slides                   : 19
```

Footprinting – Metadatos

- Otra forma de extraer información de la imagen es…
- … analizando el contenido de la imagen mediante una **inspección visual**.

Índice

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- **Técnicas de recogida de información**.
  - Footprinting.
  - **Fingerprinting.**
- Anonimato.

Fingerprinting

Universidad Rey Juan Carlos

- Se trata de una recogida de datos más específicos que permiten recopilar información sobre toda la pila TCP/IP de una red o sistema concreto.
  - Topologías, direcciones y nombres a diferentes niveles.
  - Estado de los puertos.
  - Versiones.
  - Estado de actualizaciones del software y parches del SO.
  - Listado de vulnerabilidades.
- Los datos que se recogen no son datos públicos por lo que se debe conseguir con técnicas específicas.

Fingerprinting

Universidad Rey Juan Carlos

- Existen cuatro técnicas muy extendidas:
  - Ingeniería social
  - Phishing
  - Sniffing
  - Scanning/mapping

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Consiste en basarse en la buena fe de las personas de una organización para obtener de ellas información valiosa para realizar los ataques.
- Se utilizan técnicas psicológicas y habilidades sociales.
- Mentiras elaboradas para sonsacar la información.
- Estas técnicas se llevan a cabo sobre:
  - Personal con falta de conciencia acerca del problema de seguridad informática.
  - Personal descontento.
- Y en muchos casos se aprovechan de la ausencia de políticas adecuadas.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider:
    - Generalmente el atacante tiene ciertos privilegios, a nivel de confianza, ligados a su condición de trabajador, colaborador o empleado de la organización.
    - Puede tener muchos motivos: motivos personales, laborales, venganza…
    - Suelen buscar dinero o dañar la imagen de la empresa o institución.
  - Ciberdelincuente.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente:
    - Atacante de perfil técnico con conocimientos de Hacking informático.
    - Busca obtener información de la víctima y obtener acceso a una estructura empresarial.
  - Hackers éticos.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

Universidad Rey Juan Carlos

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos:
    - Es un pentester, autorizado por la organización, que puede usar técnicas de Ingeniería Social para auditar la seguridad.
  - Estafadores o timadores.
  - Espías.

Fingerprinting – Ingeniería social

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos
  - Estafadores o timadores:
    - Personas usan la Ingeniería Social para la elección de sus víctimas.
  - Espías.

Fingerprinting – Ingeniería social

- Hay diferentes tipos de personas que utilizan la ingeniería social:
  - Insider.
  - Ciberdelincuente.
  - Hackers éticos
  - Estafadores o timadores.
  - Espías:
    - Tratan de manipular a su objetivo para que realice determinadas acciones.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
    - Un atacante obtiene acceso a un sistema utilizando la conexión de otro usuario y períodos de inactividad cuando dicho usuario no está utilizando la cuenta.
    - Se basa en seguir a un usuario autorizado mientras va pasando a zonas de acceso restringido a las que no podemos acceder.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
  - Dumpster Diving o Trashing:
    - Buscar en la basura o en lugares donde se acumulen desechos de información que podrán ser utilizados por el atacante.
    - Buscar en la basura está prohibido, pero se puede encontrar mucha información:
      - Número de teléfono, direcciones.
      - Organigramas o directorios corporativos.
      - Planos, apuntes técnicos.
      - Manuales de aplicaciones, sistemas, equipos, …
      - Esquemas que contengan estrategias empresariales.
      - Membretes, firmas, logotipos.
      - Actas de reuniones
      - Cuadrantes de vacaciones, turnos, eventos, …
      - Facturas con datos fiscales, precios, descripciones de productos…

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking:
  - Dumpster Diving o Trashing:

elmundo.es Castilla y León 24h

ESPAÑA | INTERNACIONAL | ECONOMÍA | CULTURA | CIENCIA | TECNOLOGÍA | DEPORTES | SALUD | COMUNICACIÓN | TV | MADRID | BCN

Buscar en Google en elmundo.es Hemeroteca Versión te

Portada > Castilla y León

VALLADOLID | 'EL MUNDO' LO DESVELÓ EN FEBRERO DE 2006

Multa de 60.000 euros a BBVA por el abandono de datos confidenciales en un descampado

- La Agencia de Protección de Datos sanciona la "conducta negligente" del banco
- La entidad alega que la responsabilidad corresponde a la empresa de limpieza

Actualizado sábado 19/04/2008 08:49 (CET)

ESTHER NEILA

VALLADOLID.- BBVA deberá hacer frente a una multa de 60.101,21 euros por el abandono de cientos de documentos confidenciales en un descampado anexo al polígono industrial de San Cristóbal, hecho que fue revelado por EL MUNDO en su edición del 6 de febrero de 2006.

Más de dos años después, la **Agencia de Protección de Datos** sanciona al banco por una **"clara conducta negligente"** en su obligación de custodiar información privada de los clientes, pero le impone la menor cuantía establecida para este tipo de infracciones (consideradas graves y que pueden acarrear multas de hasta 300.000 euros) al **no percibir intencionalidad** por parte de la entidad.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping:
    - Es el acto de escuchar secretamente conversaciones privadas o de otros sin su consentimiento.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping:

NSA espiaba a asistente
Angela Merkel: Wikilea

WikiLeaks publicó una lista de números telefónicos alemanes que Estados Unidos vigiló conexiones en la Cancillería y de asistentes Angela Merkel.

AP
08 de julio de 2015, 17:09

GOBIERNO >

El Gobierno denuncia que los móviles de Sánchez y Robles fueron espiados con el programa Pegasus

Los atacantes extrajeron 2,6 gigas de datos del teléfono del presidente y nueve megas de la ministra de Defensa. El Ejecutivo no sabe aún cuál es la información robada y su grado de sensibilidad

ESCÁNDALO

Multa a LaLiga de fútbol por usar el móvil de 50.000

ar

su

iado que
ñola de

El presidente de LaLiga, Javier Tebas EFE

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing:
    - Mirar de manera disimulada para conseguir la información que se busca.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping:
    - Aprovechar que un compañero de trabajo no está en su puesto y no ha bloqueado el equipo.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting:
    - Dejar un dispositivo, que tiene un malware, y que la víctima por curiosidad conecte ese dispositivo en su equipo.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting
  - Bribing:
    - Sobornar a un empleado de la empresa para que este nos facilite la información.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Existe una gran variedad de ataques que usan la Ingeniería social:
  - Piggybacking
  - Dumpster Diving o Trashing
  - Eavesdropping
  - Shoulder Surfing
  - Office Snooping
  - Baiting
  - Bribing
  - Ingeniería Social Inversa:
    - Se trata de poner un cebo y esperar a que la víctima pique.

Ingeniería Social – Ataques

Universidad Rey Juan Carlos

- Ejemplo de ingeniería Inversa:
  - La DEA (*Drug Enforcement Administration*) creó un perfil falso en Facebook usando las imágenes que obtuvieron de un móvil requisado a una detenida. La suplantación pretendía servir de trampa a otros traficantes.

Fingerprinting

- Existen cuatro técnicas muy extendidas:
  - Ingeniería social.
  - Phishing.
  - Sniffing.
  - Scanning/mapping.

Phishing

Universidad Rey Juan Carlos

- El atacante se hace pasar por otra persona o entidad en la cual el atacado confía.
- Tiene puntos en común con la Ingeniería Social.
- El caso típico persigue extraer información confidencial enviando a todas las víctimas potenciales una comunicación confiable y legítima solicitándoles esa información.
- Aparecen conceptos como:
  - Spear phishing: si el objetivo es un determinado grupo de personas.
  - Whaling: si el objetivo son los directivos de la organización.
- Tipos:
  - Smishing: usando SMS, o apps de mensajería como Telegram o Whatsapp.
  - Phishing: usando el correo electrónico.

Sniffing

Universidad Rey Juan Carlos

- Es una técnica que permite capturar todos los datos que circulan por una red de área local.
  - No es necesariamente maliciosa.
- Se utilizan los sniffers: software que configura las tarjetas de red en modo promiscuo, y que soporta los protocolos de interés y proporciona mecanismos de filtrado adecuados.
- Su alcance depende de los dispositivos de conmutación o segmentación que se utilizan en la red, de su correcta configuración, de la forma de acceso.
- Es una técnica típica para conseguir contraseñas.

Scanning/Mapping

Universidad Rey Juan Carlos

- El scanning trata de analizar a través de diferentes herramientas el estado de una determinada red y de los dispositivos ubicados en ella.
- Existen diferentes tipos dependiendo del nivel de profundidad y del objetivo del análisis:
  - Escáner de puertos (NMAP, NETCAT, SUPERSCAN, Metasploit).
  - Escáner de vulnerabilidades (Nessus)

Índice

- Introducción.
- Técnicas de Hacking.
- Fases de un ataque.
- Técnicas de recogida de información.
- **Anonimato.**

Anonimato

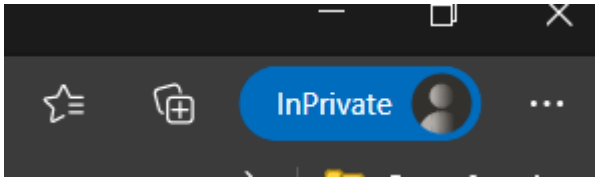
Universidad Rey Juan Carlos

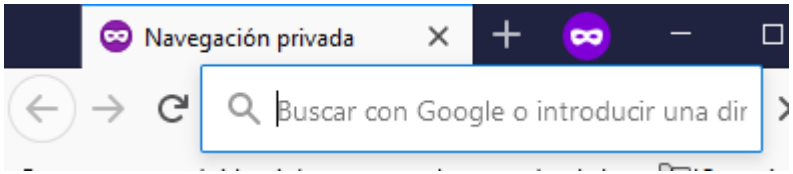
- El anonimato es fundamental desde el punto de vista del atacante por dos aspectos fundamentales:
  1. Ocultar su identidad desde las fases iniciales del ataque.
  2. Borrar sus huellas para dificultar posibles análisis forenses.

- Generalmente, se utilizan tres técnicas diferentes:
  - Anonimato físico: acceso mediante Wifis abiertas.
  - Anonimato por uso de **bouncer**: sistema sobre el que el atacante tiene un control total y desde el cual realiza el ataque.
  - Anonimato por uso de proxy.

Anonimato

- Todos los navegadores disponen de un modo de navegación de incógnito (no fiarse nunca):





Anonimato

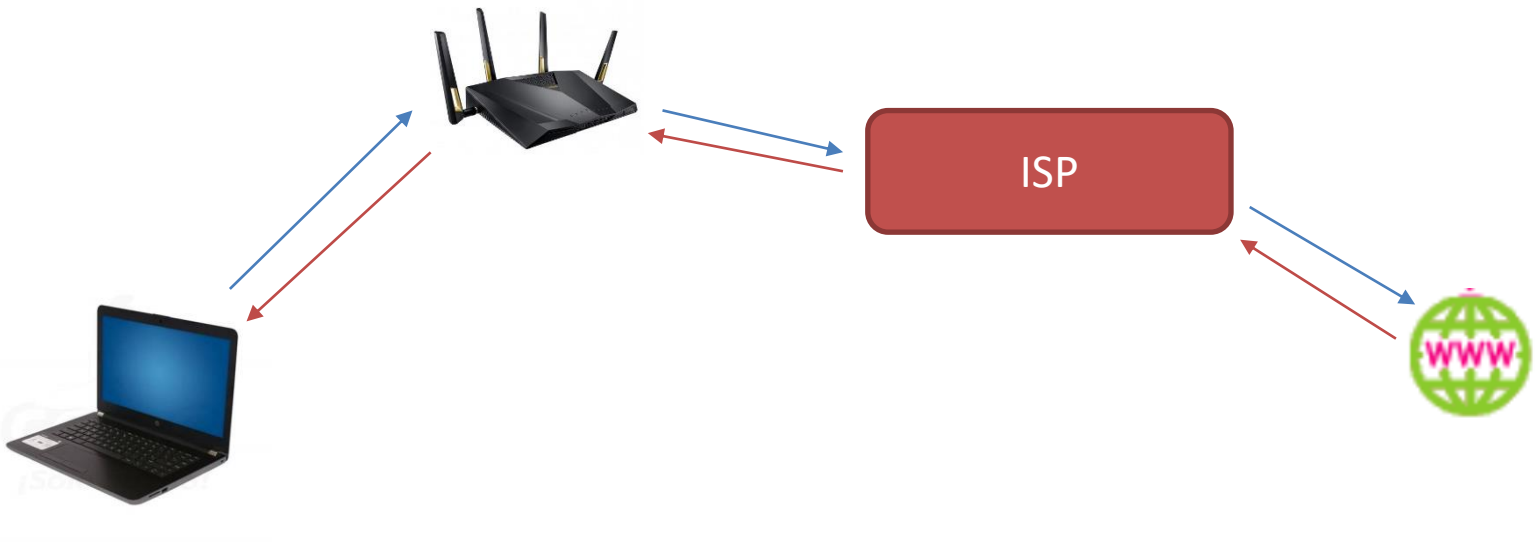
- Aunque también existen otras maneras:
  - Usar TAILS.
    - Es un SO de software libre basado en Debian.
    - Fuerza que todas las conexiones salientes sean a través de la red TOR.
  - Usar la red TOR: The Onion Router.

Anonimato: TOR

- El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional.
- TOR es una red que implementa una técnica llamada *Onion Routing*, diseñada para proteger las comunicaciones en la Marina de los Estados Unidos.
- La idea es cambiar el enrutado tradicional de Internet para garantizar el anonimato y la privacidad de los datos.

Anonimato: TOR

- En enrutado clásico:



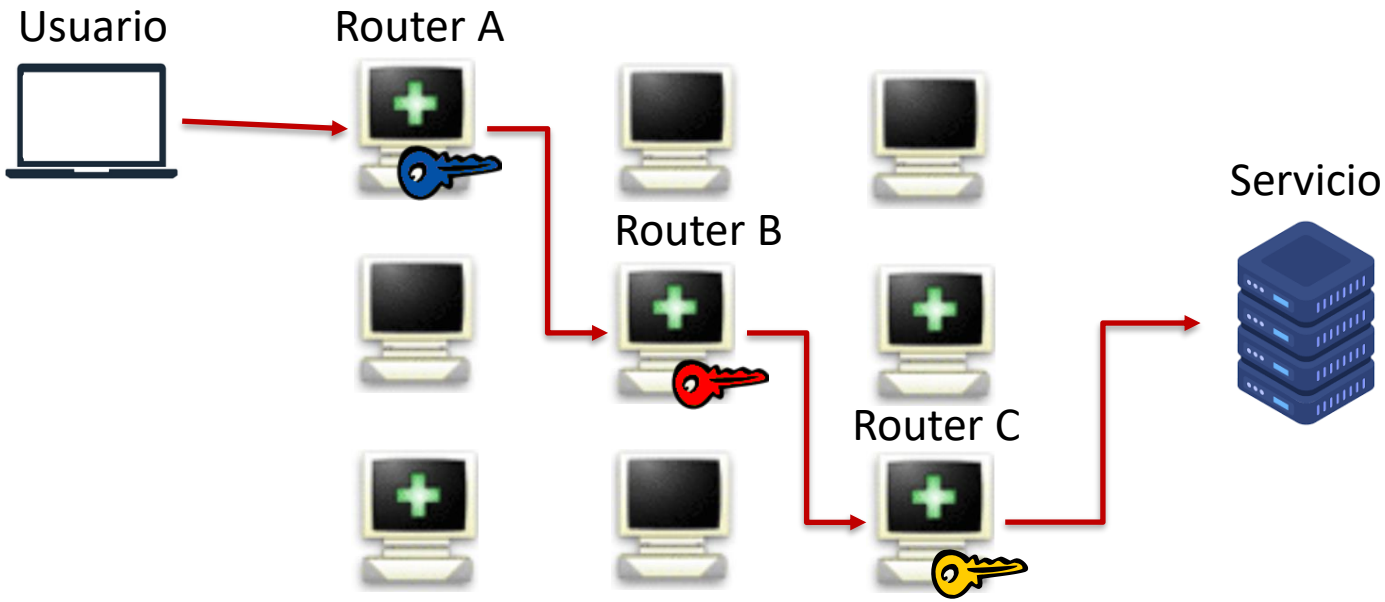
- Si alguien intercepta el paquete de datos (MiM) sabe de dónde vienen y a dónde van.

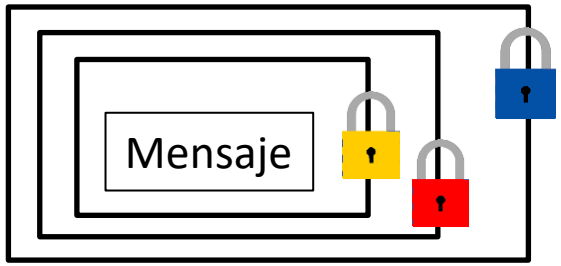
Anonimato: TOR

- Onion Routing: consiste enviar los datos por un camino no directo utilizando nodos.

- El nodo A quiere mandar un mensaje al nodo B.
- Calcula una ruta más o menos aleatoria al destino.
- Después consigue las claves públicas de todos los nodos intermedios usando un directorio de nodos.
- Va cifrando el mensaje por “capas”.

Anonimato: TOR





Anonimato: TOR