**Práctica Phishing**

**Qué es**

**Definición:**

*Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace)*

**Método**:

*Para realizar el engaño, habitualmente se hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. También mediante la adulación de la víctima, explotando su intrínseca vanidad o necesidad de ser reconocido, baja autoestima, o una persona que busca trabajo. Por ejemplo, enviando correos electrónicos o mostrando publicidades a la víctima diciéndole que ha ganado un premio y que siga un enlace para recibirlo, siendo aquellas promesas falsas (un cebo). A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes.*

**Origen:**

*El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión a utilizar un cebo y esperar a que las víctimas "muerdan el anzuelo".*

**Tipos:**

*\* Phishing general, phishing tradicional, Bulk Phishing o Spray and pray. Consiste en la emisión masiva de correos electrónicos a usuarios. Estos correos suplantan a entidades de confianza (ejemplo bancos) y persiguen el engaño del usuario y la consecución de información. Por ejemplo en el mensaje se incluyen enlaces a dominios maliciosos. Para camuflar estos enlaces es habitual*

*que el texto del enlace sea la URL correcta, pero el enlace en sí apunte al sitio malicioso.*

*\* Vishing. Es similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica. El término deriva de la unión de dos palabras en inglés: ‘'voice'’ y ‘'phishing’'.*

*\* Smishing. Es similar al phishing tradicional pero el engaño se produce a través mensajes de texto ya sean por SMS o mensajería instantánea (como WhatsApp).*

*\* URL Phishing. Se trata de engañar al usuario haciendo que una URL de un sitio malicioso parezca la de un sitio confiable. A ellas a veces se accede de forma inadvertida al escribir nombres de dominio mal escritos que están muy cerca del dominio legítimo, o siguiendo un enlace malicioso que parece correcto, o por engaños al usar caracteres unicode parecidos difícilmente detectables.*

*\* Whaling. Se diferencia de los otros tipos de intentos de phishing en que el objetivo son personas importantes como por ejemplo ejecutivos de alto rango. Las solicitudes de información contenidas en el ataque están más adaptadas a la persona concreta.*

(Fuente: Wikipedia, https://es.wikipedia.org/wiki/Phishing)

**Qué se necesita**

**Atacante:**

\* Máquina virtual con Windows o Linux (Ip estática)

\* Servidor DHCP

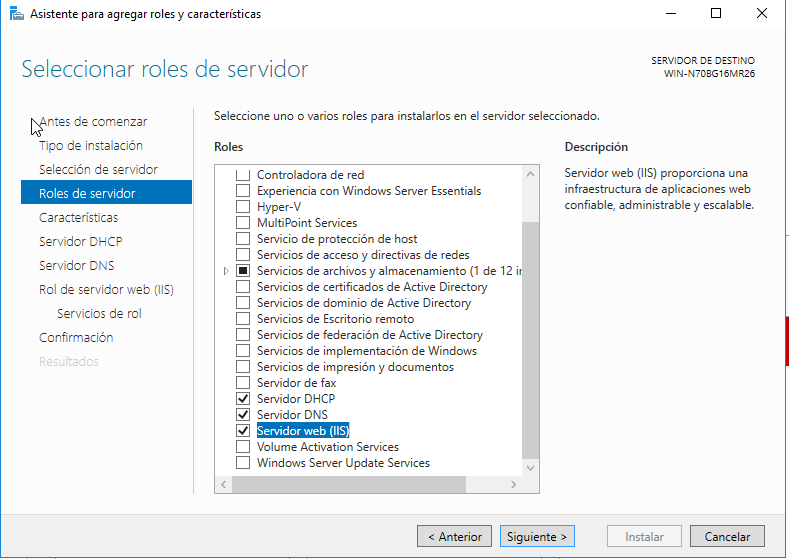
\* Servidor DNS

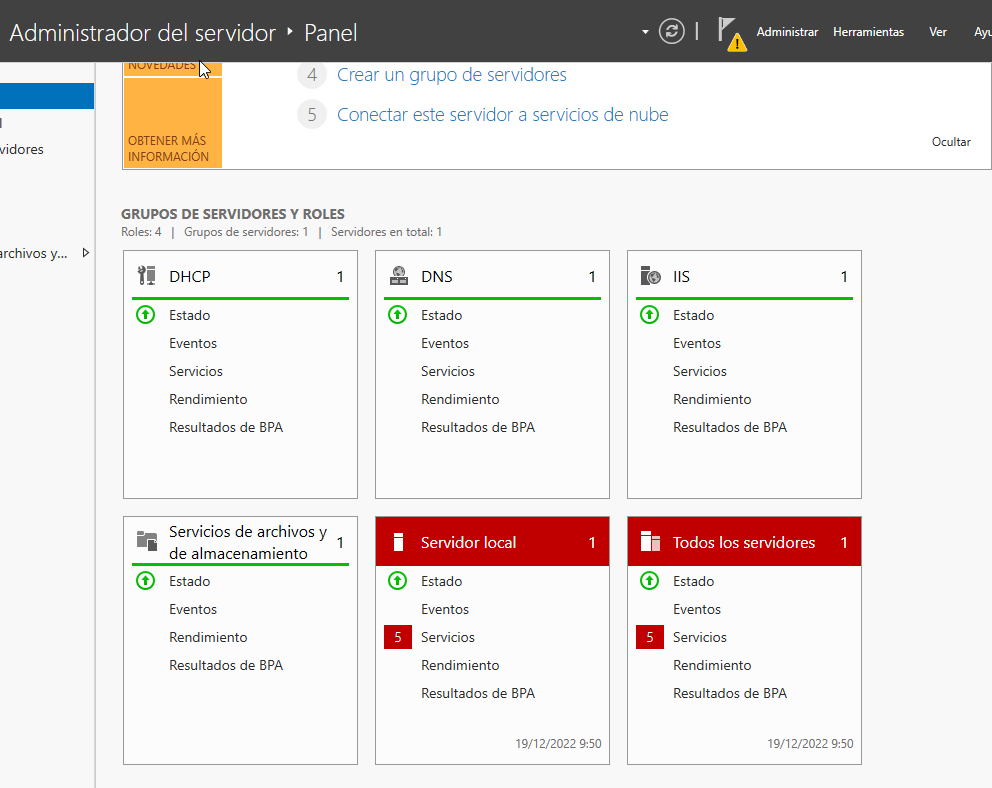
\* Servidor WEB con PHP

\* Conexión en red con la víctima

\* (Opcional: Servidor de correo, Servidor de bases de datos)

1. **ADMINISTRAR, AGREGAR ROLES Y CARACTERÍSTICAS: DHCP, DNS, IIS (dentro está el servidor de correo y el web) → instalación de todas y reinicio, aquí probamos que están todos de alta:**

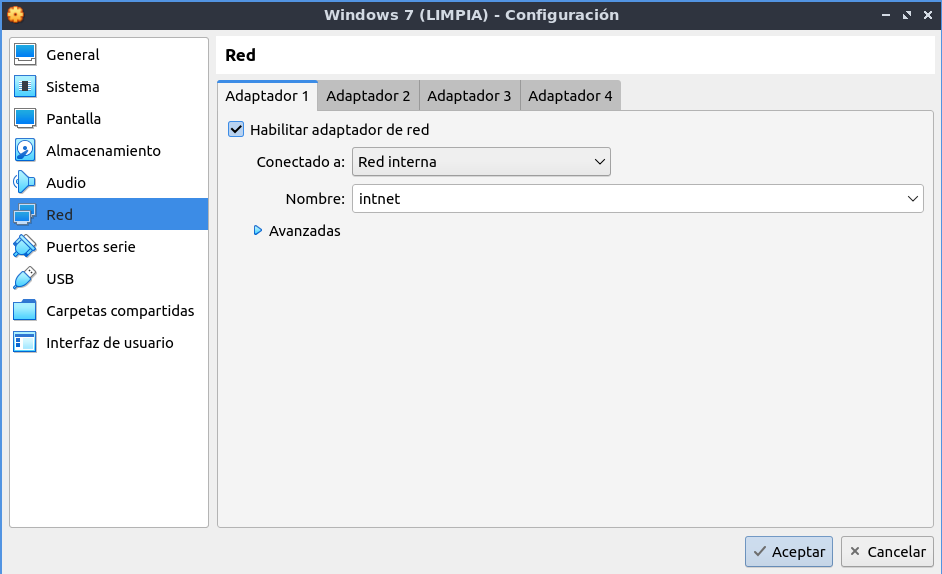
****

**Víctima:**

\* Máquina virtual con Windows o Linux (Ip dinámica)

\* Conexión en red por DHCP con el atacante

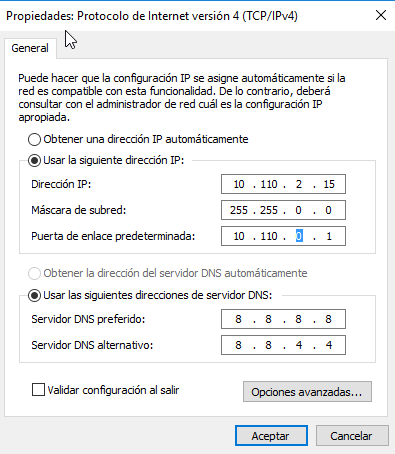
**RED INTERNA W7:**

****

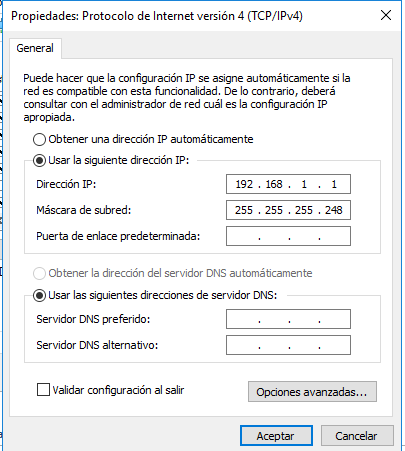
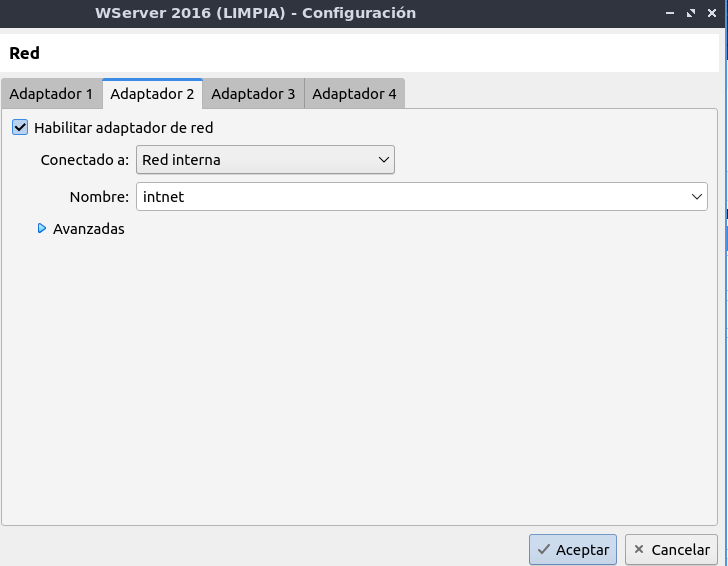
**Cómo es el proceso (Trabajo)**

- Instalar 2 máquinas en VirtualBox en red interna (sólo comunicación entre ellas) 1 Atacante con IP fija (Windows o Linux) 1 Víctima con IP dinámica (Windows o Linux)

**IP FIJA EN EL WSERVER, RED PUENTE:**

****

**RED INTERNA WSERVER:**

****

- En el "atacante" instalar un servidor DHCP

\* Linux manual (isc-dhcp-server)

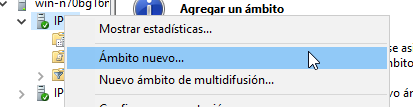
\* Linux web (webmin)

\* Windows server

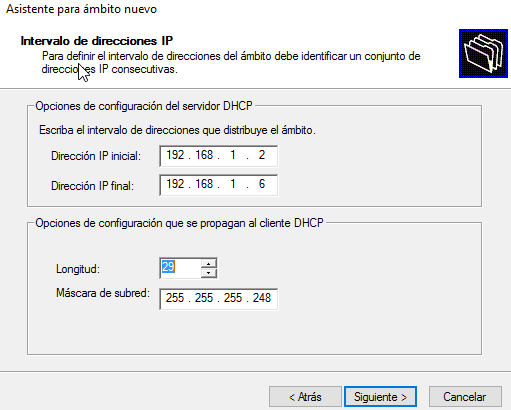
**Configurar que de como servidor DNS la ip del Atacante**

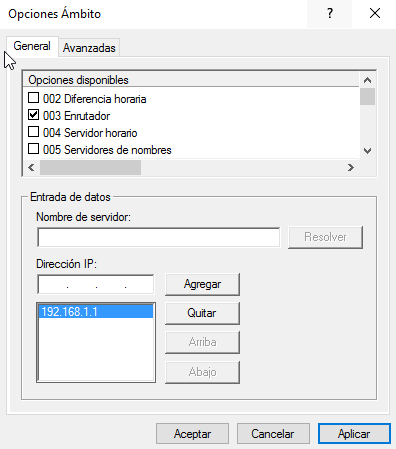
**CONFIGURAR DHCP:**

**HERRAMIENTAS → DHCP –>IPV4→ÁMBITO NUEVO**

****

**excluimos la primera ip que será la de la red interna del servidor**

****

****

**EL SERVIDOR DNS DEL CLIENTE VA A SER EL PROPIO SERVIDOR DHCP PARA PODER HACER EL ATAQUE**

**w7:**

****

- En el "atacante" instalar un servidor DNS

\* Linux manual (bind9)

\* Linux web (webmin)

\* Windows server

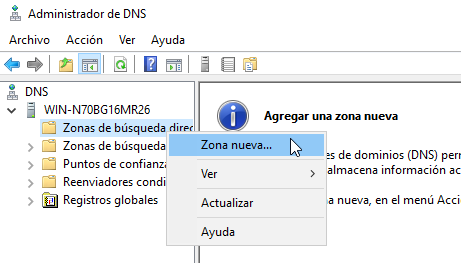
**Configurar que www.banco.es apunte a la ip del Atacante**

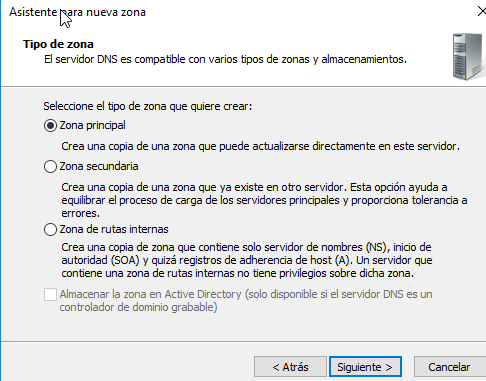
**- En el "atacante" instalar un servidor WEB con PHP**

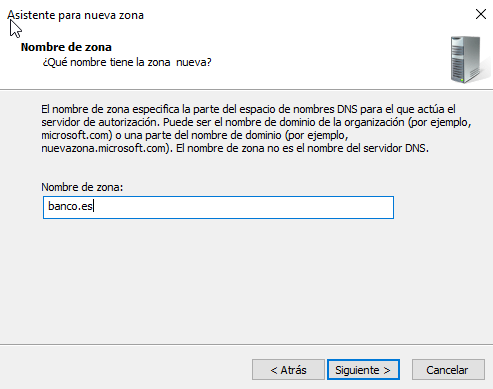
\* Linux manual (apache2)

\* Windows server

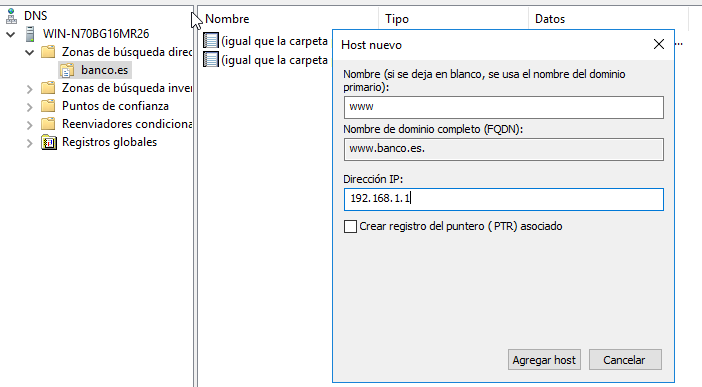
**HERRAMIENTAS → DNS**



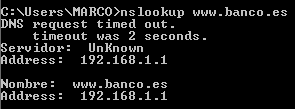




**Registro tipo A:**

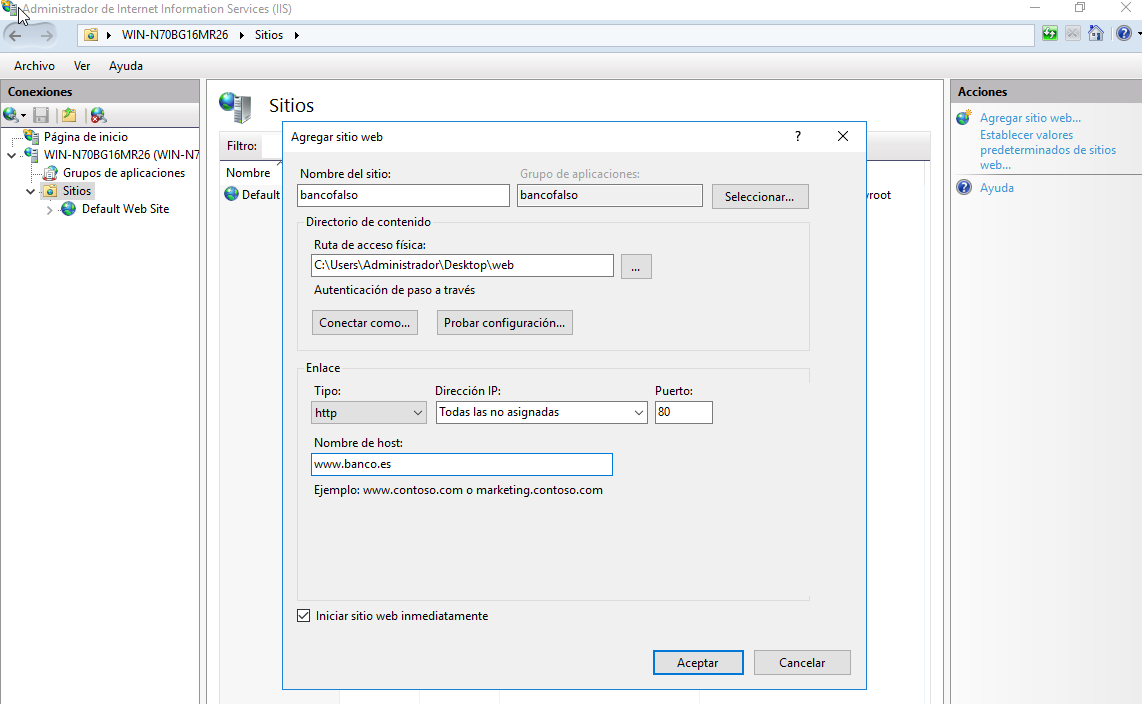
****

**MÁQUINA CLIENTE:**

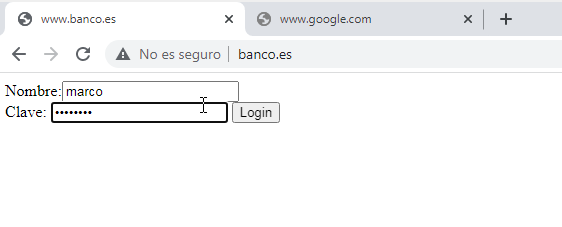


- En el servidor WEB crear 2 páginas

\* Página inicial (index.htm) con la apariencia de un banco que solicite usuario y contraseña y los envíe al servidor.



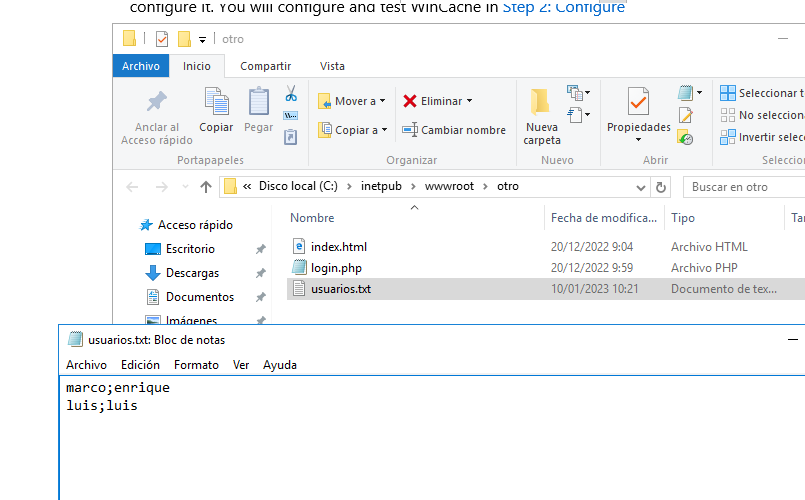
**CLIENTE:**

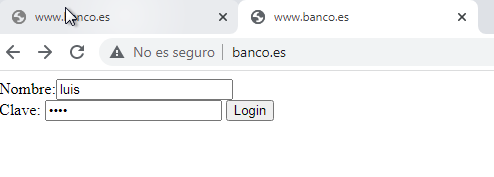
****

****

**Hay que dar permisos a ambos para que puedan ejecutar ficheros.**

<https://learn.microsoft.com/en-us/iis/application-frameworks/scenario-build-a-php-website-on-iis/configuring-step-1-install-iis-and-php> →INSTALACIÓN PHP

****



**\* Página en PHP (login.php) que reciba los datos de usuario y contraseña y los almacene en un fichero.**

- (Opcional 1)

\* Instalar un servidor de correo (Linux: postfix+dovecot; Windows Server) \* Enviar un email a la víctima con el enlace www.banco.es que envíe a la dirección IP del servidor WEB

<a href="IP\_del\_Servidor"> www.banco.es </a>

Ej. <a href="192.168.1.2"> www.banco.es </a>

- (Opcional 2)

\* Enviar por email los datos recogidos en PHP

- (Opcional 3)

\* Guardar en una Base de Datos la información recogida en PHP

**Ayuda**

**Páginas:**

\* index.htm

<form action="login.php" method="post">

Nombre: <input type="text" name="nombre"> <br>

Clave: <input type="password" name="clave"> <br>

<input type="submit" value="Login">

</form>

\* login.php que guarde la información que recibe en un fichero "usuarios.txt" <?php

$informacion=$\_POST["nombre"].";".$\_POST["clave"].PHP\_EOL;

$fichero=fopen("usuarios.txt","a");

fputs($fichero,$informacion);

fclose($fichero);

?>