### Index.html

```
<html>
    <head>
    <meta charset="utf-8"/>
   <meta name="author" content="Tu nombre"/>
    <title>Redes en Cloud y Ciberseguridad</title>
    </head>
<style>
   img:hover {
    filter: blur(4px);
    transition:.3s all;
    border-radius: 10%;
   }
   .titulo {
      font-size: xx-large;
     text-align: center;
     color: #fff;
     background-color: #000033;
    .table {
    width: 100%;
   }
    .fa {
      padding: 10px;
     font-size: 30px;
     width: 20px;
     text-align: center;
     text-decoration: none;
     margin: 5px 2px;
     border-radius: 50%;
   }
    .fa:hover {
        opacity: 0.7;
    .fa-facebook {
     background: #3B5998;
      color: white;
   }
    .fa-twitter {
     background: #55ACEE;
      color: white;
    .fa-youtube {
     background: #bb0000;
```

```
color: white;
}
.fa-instagram {
  background: #125688;
  color: white;
}
.ventana {
 position: fixed;
 left: 0;
 top: 0;
 width: 100%;
 height: 100%;
 background-color: rgba(0, 0, 0, 0.5);
 opacity: 0;
 visibility: hidden;
 transform: scale(1.1);
transition: visibility Os linear 0.25s, opacity 0.25s Os, transform 0.25s;
}
.contenido-ventana {
 position: absolute;
 top: 50%; left: 50%
 transform: translate(-50%, -50%);
 background-color: white;
 padding: 1rem 1.5rem;
 width: 24rem;
 border-radius: 0.5rem;
}
.boton-cerrar {
float: right;
width: 1.5rem;
 line-height: 1.5rem;
 text-align: center;
 cursor: pointer;
 border-radius: 0.25rem;
background-color: lightgray;
}
.boton-cerrar:hover {
 background-color: darkgray;
}
.mostrar-ventana {
opacity: 1;
 visibility: visible;
transform: scale(1.0);
transition: visibility Os linear Os, opacity 0.25s Os, transform 0.25s;
}
.cuadrado{
 padding:15px;
 opacity: 0.85;
 margin:10px;
 background-color: #ccffff;
 color: black;
 margin-right:auto;
```

```
margin-left:auto;
    margin-top:auto;
    margin-bottom:auto;
   }
</style>
<body background="imagenes/ladrillos.jpg">
   <header>
   <h1 class="titulo" font-family="sans-serif" style="text-align:center" >Redes
en Cloud y Ciberseguridad</h1>
   </header>
   <hr>>
   <hr>>
   <br>
   <br>
   <br>
   <hr>
   <hr>
   <br>
   <br>
<a href="reto1.html"><img src="imagenes/crunchyroll.jpg" align="left"
vspace="25" hspace="50" style="border-radius: 10%" width="350" height="200"></a>
<a href="man.html"><img src="imagenes/man.jpg" align="center"</pre>
vspace="25" hspace="50" style="border-radius: 10%" width="350" height="200"></a>
<a href="Intro_Reto4.html"><img src="imagenes/crypto_intro1.jpg"
align="right" vspace="25" hspace="50" style="border-radius: 10%" width="350"
height="200" ></a>
   <a href="Introduccion_Reto2"><img src="imagenes/rick_morty_intro.jpg"
align="right" vspace="25" hspace="50" style="border-radius: 10%" width="350"
height="200" ></a>
   <a href="xss.html"><img src="imagenes/xss.png" align="right" vspace="25"
hspace="50" style="border-radius: 10%" width="350" height="200" ></a>
   <img src="imagenes/PopUpFinal.png" width="200" height="200" class="trigger">
   <div class="ventana">
   <div class="contenido-ventana">
   <span class="boton-cerrar">&times;</span>
   <h1>Esta web se trata de un proyecto de fin de Grado Superior de ASIR en la
cual existen varios retos, pulsa cualquiera de
   las imágenes para ir a su explicación.</h1>
   </div>
   </div>
   <script type="text/javascript">
   var modal = document.querySelector(".ventana");
   var trigger = document.querySelector(".trigger");
   var closeButton = document.querySelector(".boton-cerrar");
   function toggleModal() {
       modal.classList.toggle("mostrar-ventana");
   }
   function windowOnClick(event) {
```

```
if (event.target === modal) {
       toggleModal();
   }
   }
   trigger.addEventListener("click", toggleModal);
   closeButton.addEventListener("click", toggleModal);
   window.addEventListener("click", windowOnClick);
   </script>
<hr>>
<footer>
   <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-</pre>
awesome/4.7.0/css/font-awesome.min.css">
       <a href="https://www.facebook.com/iesleonardodavincimadrid"
class="fa fa-facebook"></a>
                  <a href="https://twitter.com/informaticaldv" class="fa fa-
twitter"></a>
                  <a href="https://www.youtube.com/user/iesleonardoinfo"</pre>
class="fa fa-youtube"></a>
                  <a href="https://www.flickr.com/photos/98165337@N02/albums/"
class="fa fa-instagram"></a>
              </div>
</footer>
</body>
</html>
```

# **Reto 1: Crunchyroll**

```
<!DOCTYPE html>
<html >
<head>
  <meta charset="utf-8"/>
</head>
<style>
.table {
  width: 75%;
  }
.degradado{
  background: linear-gradient(180deg, #B9B9C8 , white);
  background-repeat: no-repeat;
}
</style>
<!-- background-color:rgba(255,0,0, 0.4); -->
<body class="degradado">
<!-- Titulo #E4E4EE -->
```

```
<h1> &nbsp;&nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
          
                                                                                                                                                                                                                                                                                                                                                    &
1: Crunchyroll</h1><hr>
<!-- Explicacion -->
>
      <FONT SIZE=5><b>Introducción:</b> En el mundo actual en el que nos
movemos las habilidades en la informatica y sobre todo las habilidades en cuanto
a la ciberseguridad son indispensables, especialmente para las grandes empresas
que disponen de cientos de servidores alojados en diferentes partes del mundo y
que son atacados casi de manera diaria. Por eso en este pequeño reto os
explicamos de una manera muy basica como es posible tomar el control de una
maquina cuando esta no esta bien configurada o los permisos de ciertos archivos
no estan bien configurados.
        <img src="imagenes/crunchyroll.png" align="right" height="325"</pre>
width="650" style="border-radius: 20%;">
     <br/><b>Escenario:</b> Te encuentras en las oficinas de Crunchyroll, empresa
dedicada a la distribución legal de anime. Has decidido a ir allí para una
entrevista de trabajo. Como reto para superar la entrevista y ver que tienes
conocimientos suficientes para cubrir el puesto ofrecido, te proponen conseguir
vulnerar una maquina virtual, en caso de conseguirlo el puesto será tuyo.
      <b>Objetivo:</b> El chico de relaciones públicas te explica lo
siguiente:
      <01>
        sencillo solo tienes que conseguir una bandera que se encuentra
en el usuario root.
      </01>
      <b>Consejos:</b>
      < 10>
        Sería bueno que usases un sistema operativo como Kali o Parrot.
        servidor esta alojado en internet no en una red local.
      </01>
      <br/><b>Pistas:</b> Como le has caído bien al entrevistador te da un par de
pistas para que no estés muy perdido.
      <01>
        Seguramente los nombres de usuarios tengan que ver con personajes de
animes.
        Creo recordar que el que hizo la maquina mencionó algo de
escenografía pero no me acuerdo con que programa lo hizo.
      </01>
      <br/><b>Último apunte:</b> Espero que disfrutes del reto y sobre todo que
puedas finalizarlo para conseguir el puesto de trabajo.
      Una última cosita... la ip de la máquina es 51.144.174.75
    </FONT>
    </body>
</html>
```

### **Reto 2: Rick & Morty**

```
<!DOCTYPE html>
<html >
<head>
  <meta charset="utf-8"/>
</head>
<style>
.table {
  width: 75%;
  }
.degradado{
  background: linear-gradient(180deg, #7FFFD4 , white);
  background-repeat: no-repeat;
}
<!-- background-color:rgba(255,0,0, 0.4); -->
<body class="degradado">
<!-- Titulo #E4E4EE -->
  <h1> &nbsp;&nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
         
                                                                                                                                                                                                                                                                                                                                                    &
Rick & Morty</h1><hr>
<!-- Explicacion -->
<img src="imagenes/rick.png" align="right" height="700" width="400">
      <FONT SIZE=5><b>Introducción:</b> 
        <!-- <img src="imagenes/crunchyroll.png" align="right" height="325"
width="650" style="border-radius: 20%;"> -->
         Dentro de la ciberseguridad, el juego CTF (Capture The Flag) es muy
común, puesto que nos permite aumentar nuestras capacidades informáticas tanto
de defensa, como de ataque. Así mismo, hay diferentes tipos de
             CTF y en este reto, vamos a desarrollar la 'Esteganografía', que
consiste en encontrar, mediante la utilización de ciertas herramientas,
información oculta, dentro de una URL o incluso en una imagen. 
      <b>Escenario:</b> 
        Tu nombre es Rick Sánchez, perteneces a la Tierra C-137 y tu misión
es encontrar a Evil Morty, que en este caso, está escondido en algún punto del
Mediante el uso de diferentes técnicas informáticas, podrás conseguir descubrir
el paradero de Evil Morty, antes de que éste decida destruir la Tierra C-137.
<b>Objetivo:</b>
      <01>
```

```
Debes llegar al final del reto, siguiendo poco a poco el rastro
de Evil Morty.
     </01>
     <b>Consejos:</b>
     < 10>
       ¡Cuidado! Evil Morty tratará de despistarte, intenta centrarte en
la misión y no irte por las ramas.
       Deberás utilizar para la mayoría de retos Google Chrome o en su
defecto, Microsoft Edge.
     </01>
     <b>Pistas:</b>
     <01>
       ¡Ninguna! Sólo ante el peligro Rick, como siempre.
     </01>
     <b>Último apunte:</b>
     Esperamos que disfrutes del reto, igual que disfrutamos nosotros
realizándolo. Mucha suerte Rick Sánchez, no será fácil atrapar a Evil Morty,
pero con esfuerzo, lograrás tu misión.
     <a href="http://52.137.32.181"> Pulsa aquí para comenzar el reto </a>
</FONT>
   </body>
</html>
```

#### Reto 3: Man in the middle

```
<!DOCTYPE html>
<html >
<head>
  <meta charset="utf-8"/>
</head>
<style>
.table {
  width: 75%;
  }
.degradado{
  background: linear-gradient(180deg, #008B8B , white);
  background-repeat: no-repeat;
}
<!-- background-color:rgba(255,0,0, 0.4); -->
<body class="degradado">
<!-- Titulo #E4E4EE -->
```

```
<h1 style="color:#99bbff"> &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
        
          
the middle</h1><hr>
<!-- Explicacion -->
>
     <FONT SIZE=5><b style="color:#6699ff">Introducción:</b> Hoy en día
casi todo el mundo poseemos un móvil o un ordenador. Cuando nos encontramos
     en nuestro hogar, tenemos la tranquilidad de nuestro acceso wifi seguro,
pero cuando andamos de aquí para allá y
     queremos ahorrar datos, a veces nos surge la tentación de conectarnos a
redes abiertas en la calle o centros comerciales.
     Este es un craso error, porque no sabemos quién ha creado ese acceso o
quién esta espiando su tráfico de red. A continuación,
     vas a comprobar porqué solo debes conectarte a redes seguras. Hay una
bandera escondida en algún lugar y debes encontrarla. Tienes pensar que en vez
de una bandera,
     podrían ser datos personales o económicos, e incluso datos por los que
puedan llegar a extorsionarte.
      <img src="imagenes/manin.png" align="right" height="325" width="650"</pre>
 style="border-radius: 20%;">
     <b style="color:#3377ff">Escenario:</b> En casa nos aburrimos, acudimos
a un centro comercial a dar un paseillo, después de varias
     vueltas, observamos que el lugar esta lleno, y como somos gente curiosa,
cogemos nuestro dispositivo y buscamos redes,
     cómo no, observamos una red abierta sin contraseña y accedemos a ella.
     <b style="color:#0055ff">Objetivo:</b> Comprueba tu mismo, si es verdad
que se pueden obtener datos de una red desconocida:
     <01>
       Escanea la red y verifica que equipos tienes alrededor.
       Envenena la red.
       Realiza un sniffing de contraseñas.
       Susca la bandera.
     </01>
     <br/><br/>b style="color:#0044cc">Consejos:</b>
       Susca en la máquina que se te proporciona aplicaciones que analicen
la red y los protocolos en el pc.
       Si necesitas descargar algún programa extra, hazlo.
     </01>
     <br/><b style="color:#003399">Pistas:</b>
       si escoges el programa correcto no tendrás problema en resolver todo
ésto, todo depende de tus conocimientos.
     </u1>
     <b style="color:#002266">Ultimo apunte:</b><br> <br>Disfruta del reto y
recuerda que es educativo. Sólo se intenta dejar ver
```

```
los peligros a los que estamos sometidos hoy en día con nuestros dispositivos conectados a internet.<br/>
br><br>> Descarga la máquina desde el siguiente enlace : <a href="https://mega.nz/folder/7zpki]xI#iLWkoKXJruBFRVToabQF8A"><h4 style="color:red;" align="center">Mega<h4></a><br/>
</font>

</body>
</html>
```

## Reto 4: Criptografía

```
<!DOCTYPE html>
< html >
<head>
  <meta charset="utf-8"/>
</head>
<style>
.table {
  width: 75%;
  }
.degradado{
  background: linear-gradient(180deg, #cc99ff , white);
  background-repeat: no-repeat;
}
</style>
<!-- background-color:rgba(255,0,0, 0.4); -->
<body class="degradado">
<!-- Titulo #E4E4EE -->
  <h1> &nbsp;&nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
          
                                                                                                                                                                                                                                                                                                                                                    &
4: Criptografía</h1><hr>
<!-- Explicacion -->
<FONT SIZE=5><b>Introducción:</b> 
src="imagenes/crunchyroll.png" align="right" height="325" width="650"
style="border-radius: 20%;"> -->
         Como bien hemos visto con los anteriores retos, hay diferentes tipos
de retos CTF, como bien puede ser la Esteganografía o, en este caso, la
criptografía. Los retos suelen consistir en utilizar diferentes técnicas para
desencriptar/encriptar cierta información. En nuestro caso, vamos a hacer uso de
diferentes acertijos, para resolver el reto.
```

```
<b>Escenario:</b> 
         Eres parte del equipo de ciberseguridad de una pequeña empresa,
por lo que tu jefe, quiere que aprendas más acerca de la criptografía, por lo
que te plantea una serie de retos.
     <b>Objetivo:</b>
     <01>
       Tu objetivo principal es resolver los retos en el menor tiempo
posible, siguiendo las propias reglas, además de aprender más sobre la
criptografía.
     </01>
       <img src="imagenes/enigma.png" align="right" height="455" width="650"</pre>
 style="border-radius: 20%;">
     <b>Consejos:</b>
     <01>
       Analiza detenidamente cada reto, pensando cuál podría ser la
solución final.
       Recomendamos la utilización de Paint para la resolución de los
primeros pasos.
     </01>
     <b>Pistas:</b>
     < 10>
       En el segundo desafío, deberás empezar el recorrido, desde abajo
a la izquierda... ¿O no?
     </01>
     <b>Último apunte:</b>
     Google siempre te va a ayudar a encontrar la información pertinente.
¡Mucha suerte!<a href="http://52.137.32.181/Reto2/"> Pulsa aquí para
comenzar el reto </a>
     </FONT>
   </body>
</html>
```

#### **Reto 5: XSS Attack**

```
background-repeat: no-repeat;
}
</style>
<!-- background-color:rgba(255,0,0, 0.4); -->
<body class="degradado">
<!-- Titulo #E4E4EE -->
 <h1 style="color:#d5ff80"> &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
          
         
Attack</h1><hr>
<!-- Explicacion -->
<ht>
     <FONT SIZE=5><b style="color:#c4ff4d">Introducción:</b> Existen
millones de páginas web, las hay de muchos tipos y para muchos propositos
diferentes.
     hay algo que muchas tienen en común, que ofrecen un acceso tanto para
usuarios como para el administrador de la misma. Para evadir este tipo de acceso
existe un tipo de ataque
     llamado "Cross Site Scripting". Existen dos tipos de este mismo ataque
pero nos vamos a centrar en el almacenado.
   >
     <br><b style="color:#b3ff1a">Escenario:</b> Nos encontramos frente a
una página web de tipo blog, en la que observamos varios post,
     un acceso para el administrador y un apartado con un formulario para
escribir comentarios.
      <img src="imagenes/xss2.png" align="right" height="325" width="650"</pre>
 style="border-radius: 20%;"><br/>
     <b style="color:#99e600">Objetivo:</b> Ejecuta un ataque xss a partir
de los siguientes pasos:
     <01>
       Comprueba la vulnerabilidad de la página ante ataques xss.
       Crea un página escrita en "php" para capturar el valor de una
cookie.
       Arranca un servidor "php" en tu equipo y monitoréalo.
       Inyecta código javascript en el formulario de los comentarios para
desviar el tráfico a tu servidor, con la página "php" que has creado.
       Captura la cookie con el monitoreo de tu servidor.
       Susca un programa para agregar la cookie a la página real, en tu
propio navegador.
     </01>
     <br/><b style="color:#77b300">Consejos:</b>
     <01>
       Ten clara la mecánica del xss almacenado antes de realizar éste
reto.
       Comprueba bien el código en busca de errores de sintáxis o
direcciones ip que te puedan ocasionar fallos a la hora de realizar el ataque.
si necesitas descargar algún programa extra, hazlo.
```

```
Si sigues los objetivos uno a uno, con un poco de programación
puedes resolver este reto.
     </01>
     <b style="color:#558000">Pistas:</b>
       <1i>Si dedicas 5 min a buscar en internet este tipo de ataque puede que
obtengas bastante información.
     <b style="color:#334d00">Ultimo apunte:</b><br>Disfruta del reto y
recuerda que es educativo. Ésto solo demuestra lo
fácil que sería robar nuestros datos en una página web que no esté protegida
contra este tipo de ataques.
<br>>cbr><br>Descarga las máquina desde el siguiente enlace :<br>
<a href="https://mega.nz/folder/Gvw0UagZ#w7NRWawbPqvFMFzqqAgcMQ"><h4</pre>
style="color:red;" align="center">Mega</h4></a>
</FONT>
   </body>
</html>
```