CTF FINAL

TEMA 1

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

Nuestro objetivo es rastrear a un terrorista cibernético. Para ello se nos da una primera pista, la cual se trata de un código qr, este al escanearlo nos dará la siguiente información:

Decode Succeeded

Raw text	Bienvenido agente. Has logrado acceder al contenido de la primera pista. Nuestras investigaciones indican que TOCHAMA fue visto navegando en http://gf0s.com/2014/08/20/h3-pista2-2 El codigo de acceso a la pagina es 4UGtm1#-69 Para estar en la pwner list, debes documentar cada hallazgo.
Raw bytes	40 07 34 26 96 56 e7 66 56 e6 96 46 f2 06 16 76 56 e7 46 52 e0 d0 a0 d0 a4 86 17 32 06 c6 f6 77 26 16 46 f2 06 16 36 36 56 46 57 22 06 16 c2 06 36 f6 e7 46 56 e6 96 46 f2 06 46 52 06 c6 12 07 07 26 96 d6 57 26 12 07 06 97 37 46 12 e0 d0 a0 d0 a4 e7 56 57 37 47 26 17 32 06 96 e7 66 57 37 46 96 76 16 36 96 f6 e6 57 32 06 96 e6 46 96 36 16 e2 07 17 56 52 01 39 c6 22 30 77 d1 22 00 13 33 3a b2 90 3b 34 b9 ba 37 90 37 30 bb 32 b3 b0 b7 32 37 90 32 b7 10 34 3a 3a 38 1d 17 97 b3 b3 18 39 97 31 b7 b6 90 0c f2 20 04 6f 80 8f 22 0a d0 01 f1 a0 cc b5 c1 a5 cd d1 84 c8 b4 c8 34 28 34 29 15 b0 81 8d bd 91 a5 9d bc 81 91 94 81 85 8d 8d 95 cd bc 81 84 81 b1 84 81 c1 85 9d a5 b9 84 81 95 cc 80 d1 55 1d d1 b4 c4 8c b4 d8 e4 34 28 34 29 41 85 c9 84 81 95 cd d1 85 c8 81 95 b8 81 b1 84 81 c1 dd b9 95 c8 81 b1 a5 cd d0 b0 81 91 95 89 95 cc 81 91 bd 8d d5 b5 95 b9 d1 85 c8 81 8d 85 91 84 81 a1 85 b1 b1 85 e9 9d bc b8 00 ec 11 ec 11 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	Bienvenido agente. Has logrado acceder al contenido de la primera pista.

Ahora nos dirigimos a la página que se nos indica. En dicha página se nos muestra una copia del billete de avión utilizado por el terrorista, y se nos dice que debemos de buscar el país al que se dirige y cambiarlo por la palabra destino de este enlace: http://labs.gf0s.com/DESTINO

En el billete se nos muestra que viaja a Chile, pero al introducirlo nos dice que Tomacha, el terrorista, nos ha engañado que no está ahí. Procedemos entonces a mirar los metadatos de dicha imagen y obtenemos unas coordenadas que lo sitúan en la India.

Rafael Osuna Ventura
2ºASIR

Al cambiar destino por India, nos lleva a otra página en la que nos aparece una zona restringida. Para poder entrar a dicha zona necesitamos una contraseña que se nos dice que está en dicha página.

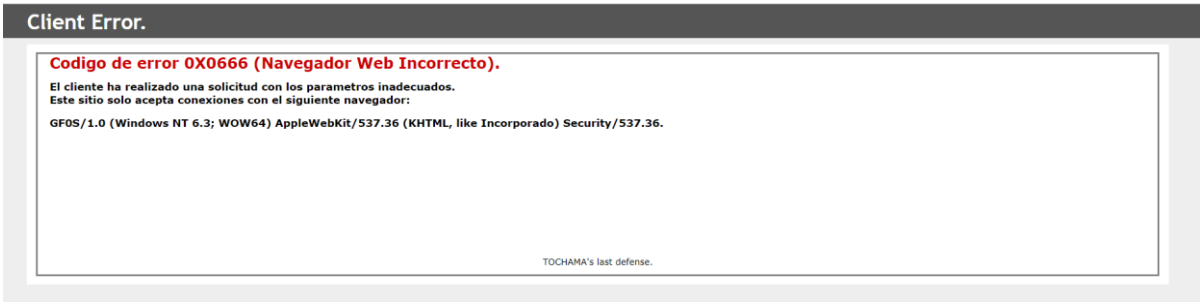
Procedemos entonces a ver el código fuente de la página, en él encontramos la sentencia para validar la contraseña y nos aparecen dos números. Tras probarlos, uno resulta ser la contraseña.

```
                        <p>Lograste identificar el destino de tochama.</p>
                        <br>
                        Tu siguiente acertijo es acceder al área restringida.<p>Todo lo que necesitas esta contenido en esta página.</p>
                        <p>Sugiero usar Chrome o Firefox.</p>
                    </header>

                    <footer>
                        <ul class="icons">

                            <li>

                            <SCRIPT>

                            eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('j i(){5 2=1;5 0=7(\'k l h n - 3 f -\',\'\');b(2<3){4(!0)9.8(-1);4(0.6()=="a"){c(\'g d!\');e.m(\'y.o\');w}2+=1;5 0=7(\'A v - u q, p r s.\',\'t\')}4(0.6()!="x"&2==3)9.8(-1);z"
"}',37,37,'pass1||testV||if|var|toLowerCase|prompt|go|history|2657|while|alert|agente|window|intentos|Bienvenido|clave|passWord|function|Introduce|la|open|correcta|html|Intenta|incorrecta|de|nuevo|Password|Clave|denegado|break|password|37463|return|Acceso'.split('|'),0,{}))


                            </SCRIPT>
<CENTER>
<br>
<FORM>
<input type="button" value="AREA RESTRINGIDA" onClick="passWord()">
</FORM>
</CENTER>

                            </li>
                        </ul>
                    </footer>
                </section>
```

Al entrar a la zona restringida nos aparecerá un enlace para descargar un. pcap. Este al abrirlo con Wireshark observamos que tiene una imagen, entonces procedemos a abrirlo con NetworkMiner y obtenemos una imagen:

Rafael Osuna Ventura
2ºASIR

Vamos a la página que se nos indica en la imagen y nos sale que nuestra solicitud no tiene los parámetros adecuados. Llegado este punto, necesito la pista del profesor para darme cuenta de que lo que hay que hacer es entrar utilizando un user agent para acceder, así como si fuéramos el terrorista cibernético.



Tras descargarnos una aplicación para realizar esto, accedemos con éxito a la página donde se nos indica que hemos superado el reto.