MISCONF CTF 2012 - Campus Party Colombia
Autor: Fernando Munoz / beford.net
Email: fernando@null-life.com

SIP:5060
Flag1
WWW-Authenticate: Digest algorithm=MD5, realm="II-9IA-G55-7AN", nonce="37b90c32"

Flag3
Marcando a la extensión 600,1 el cual es el echo demo test se obtienen unos tonos DTMF, al convertirlos de base octal a decimal en grupos de tres, se obtiene la respuesta:

```
x= "3022771311011371031171161171030631231371051141371201220601310631031240601371021251
2313113712406011606307 7"

z=''
for i in range(0, len(x), 3):
    z=z+ chr(int(x[i:i+3], 8)),
print z
```

¿YA_CONOC3S_EL_PR0Y3CT0_BUSY_T0N3?

SNMP:16100
Flag1
snmpwalk -v 2c -c public 50.116.40.66:16100
STRING: De Medellin Colombia con Amor: 8U-PLZ-J7A-63

DNS:53
Con nslookup usando el servidor dns instalado en el target, se le hace una peticion con set type=any del dominio openstackcolombia.org
y retorna Flag1 y Flag2.

Flag1
Mail addr: UU-4AR-9OA-NZ
Flag2
Registro TXT "84 84 45 88 88 88 45 80 76 65 45 56 85"
TT-XXX-PLA-8U

SVN:3690
Flag1
svn log svn://50.116.40.66/home/reto
r1 | root | 2012-06-22 15:00:26 -0300 (Fri, 22 Jun 2012) | 3 lines
Initial import, yeah, do you want another flag?

got it: UU-UUU-UUU-UU

HTTP:5566
Virtualhost: defecto
Flag1
En el readme.txt: BH-7AA-FFF-JB

Flag2
Encontrando y crackeando el archivo .htpasswd (admin:1mWKUbqjI$80gYuF0VWFL2fbf7Ea/bq1), ingresamos a la carpeta oculto y encontramos la respuesta: KO-87P-000-AG

Virtualhost: nonroot
Lugar donde se almacenaban los retos

Virtualhost: localhost
Flag1
Un regalito para subir la moral: YY-KKK-LLL-8A

Flag2
localhost:5566/cgi-bin/test
Uhmm... tienes mucha creatividad, te mereces otra FLAG: GB-LPN-8UA-01

Cisco:16010
Flag1
Welcome to my router, I'm Watching You ... P1-AP0-C0C-0D

Flag2
Se ejecuta el comando enable, la clave es bigbrother, se ejecuta el siguiente comando:
NAVAJO#>more default-running-config
...
password 7 10173D5422303546202806667D12
...

Usando http://www.ibeast.com/content/tools/CiscoPassword/decrypt.php?txtPassword=10173D5422303546202806667D12&submit1=Enviar se logra obtener la bandera: 9T-GGG-LLL-9Z

FTP:23100
Flag1
220 Welcome to 89-OIQ-A09-BV service.

Flag2
Acceder al archivo flag.txt: 93-222-111-9V

Flag3
Acceder al archivo raro

Pasándolo por varios metodos de códificacion (FERON-64, HTML encode, ESAB-46, MEGAN-35, AER-256) se obtiene la respuesta ODIO_LOS_CODIFICADORES_ONLINE

POP3:23876

Flag1
+OK Bienvenido a nuestro sistema, toma lo tuyo: IO-P0P-110-YA

Flag2
User: nonroot
Pass: nonroot
RETR 1
...
Please insert the following code into the website at http://ipv6.he.net/certification: HE-IPV-6XD-XD

Retos

aklenstra

"Factorizar" el número del reto RSA-100:
379752279369436739228088727554456278545655366381 99 *
400946909509208810306837352927614683892148997240 61
La respuesta es el MD5 del primer factor.

binario

Decompilando el binario encontramos el siguiente código:

```
...
if ( v21 <= 12.0 )
    {
      puts("So sorry, try again!");
      result = -1;
    }
    else
    {
      strcpy((char *)&v20, *(const char **)(a2 + 4));
      v5 = 84; v6 = 111; v7 = 121; v8 = 95; v9 = 79; v10 = 70; v11 = 117; v12 = 115;
      v13 = 99; v14 = 97; v15 = 105; v16 = 116; v17 = 48; v18 = 0; v28 = &v18; v27 =
0;

      while ( *(&v5 + v27) )
      {
        v4 = *(&v5 + v27++);
        putchar(v4);
      }
      result = 0;
...
```

Que traduce a la respuesta que espera el sitio: Toy_OFuscait0

binario2

Del servicio POP3 se extraen tres binarios, cada uno imprimía las siguientes frases:
1. Amar es… borrar el Windows del disco de ella.
2. Microsoft: Ustedes tienen las preguntas, nosotros los clips que bailan.
3. El dinero no hace la felicidad, pero yo prefiero llorar en una ferrari.

La respuesta son las tres frases concatenadas.

data2

Flag1
Se extrae la cadena 6H-7AA-F32-AB del archivo binario

Flag2

Se utilizan los siguientes comandos sobre la imagen:
$ affcat data2 > disk_file
$ foremost disk_file

Se extraen dos gifs que al sobreponerlos con gimp da la respuesta: crypto|steg

texto
Del servicio Cisco se extrae la url mediante el comando more unix:/flag, encontramos el texto que está en lenguaje piapoco, se traduce y se extrae la primera letra de cada palabra.

La respuesta es: ESTAFLAGESCOMORARAPEROESLAFLAGCORRECTA

Instructivo de MisConf en PDF
Usando las flags del texto guia de ejemplo:
6Y-OAN-MMM-09