CTF Ekoparty 2012
Autor: Marcelo Echeverría
Twitter: @marceloje
URL: http://emyei.immunix.com.ar/
Email: marcelo@null-life.com

DNS: 53000

Se extraen los datos del servicio DNS:

```
$ nslookup
> set port=53000
> set type=any
> ekoparty.org
Servidor:  [192.168.2.5]
Address:  192.168.2.5

ekoparty.org
      primary name server = ekoparty.org
      responsible mail addr = root.ekoparty.org
      serial  = 2
      refresh = 604800 (7 days)
      retry   = 86400 (1 day)
      expire  = 2419200 (28 days)
      default TTL = 604800 (7 days)
ekoparty.org      nameserver = localhost
ekoparty.org      internet address = 127.0.0.1
ekoparty.org      AAAA IPv6 address = ::1
ekoparty.org      text = "Mira esta FLAG: RXB-819-QAF"
ekoparty.org      text
= "RGVzY2FyZ2EgZWwgYXJjaGl2bzogRmlsM1A0cjRuNGwxejRyDQoNCkxhIHJlc3B1ZXN0YSBkZWJ
lIHNlcjogU0hBMSh1c3VhcmlvfGNsYXZlfHRpcG9oYXNoKQ0K"

localhost         internet address = 127.0.0.1
localhost         AAAA IPv6 address = ::1
```

Flag 1

Realizando fuerza bruta sobre el algoritmo de monosustitución, obtenemos la bandera: **EKO-819-DNS**

Flag 2

Decodificando la cadena en base64 obtenemos el texto:

```
Descarga el archivo: Fil3P4r4n4l1z4r La respuesta debe ser: SHA1(usuario|clave|tipohash)
```

Descargamos el archivo del servidor FTP:

```
ftp> get Fil3P4r4n4l1z4r
227 Entering Passive Mode (192,168,2,5,240,185).
150 Opening BINARY mode data connection for Fil3P4r4n4l1z4r (38225 bytes).
226 Transfer complete.
38225 bytes received in 3.95 seconds (9679 bytes/s)
```

Fil3P4r4n4l1z4r es un archivo comprimido que contiene logs de un servidor HTTP de un ataque con SQLMap.

El log original hay que arreglarlo para quitarle los registros que no sean por blind sql injection, ejemplo, quitar esta línea:
/admin/update.php?Submit=submit&id=999999.9%27+union+all+select+%28select+concat

Después hay que normalizar los datos para que cada letra esté en un bloque de texto:
information_schema.SCHEMATA),1,1)) > 48 AND
information_schema.SCHEMATA),1,1)) > 49 AND
information_schema.SCHEMATA),1,1)) > 50 AND

information_schema.SCHEMATA),2,1)) > 58 AND
information_schema.SCHEMATA),2,1)) > 59 AND
information_schema.SCHEMATA),2,1)) > 60 AND

Se obtienen los datos a través de un análisis automático, verificando que la respuesta del servidor siga un patrón, teniendo como resultado principal estos tres archivos:

- ```
  /tmp/flag
  Esta no es la flag :P
  ```

- ```
  /etc/passwd
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/bin/sh
  nonroot:x:1000:1000:nonroot user,,,:/home/nonroot:/bin/bash
  ```

- ```
  /etc/shadow
  root:$6$/Wy.oA2v$BtvDsMjdA1VFW/
  DHdj2ZxXQCsXCk9YI8F.GkQk.0Pd5k8r8556.9yh8nLRcaefBTsVKjZbmIsc60hdsSkUR1A
  0:15595:0:99999:7:::
  daemon:*:15096:0:99999:7:::
  nonroot:$6$Kp7xUGbH$kmxM3zQF1Q.KKuaLdaHDPAOcEfotCmY6qPG4v9OdOtz8803iVAC
  EJ7KIijGjA2awVOEe7itX5cyRlRh/Zwi/t1:15595:0:99999:7:::
  ```

La contraseña de root es: webmaster (root)
La respuesta es sha1("root|webmaster|SHA512"):
b51991007438370b6d833c73339f5a1c2bdf5b4b
  ```

SVN: 8080

Dado como pista el repositorio, se obtiene información del mismo con:

```
svn info svn://192.168.2.5:8080/datos/repositorio
```

Se observa la máxima revisión y se analizan con:

```
svn list -r 165 svn://192.168.2.5:8080/datos/repositorio
svn list -r 164 svn://192.168.2.5:8080/datos/repositorio
```

En la revisión 162 se descarga un archivo:

```
UA8JAKS9S8SUJS2
```

Al descomprimir este archivo, obtenemos un log de tráfico USB. Luego de analizarlo con vusb-analizer, rápidamente se observa una sesión SSH.

De acuerdo a las instrucciones del reto, la flag está contenida en un archivo, por lo que buscamos la ejecución del comando cat:

```
strings exfiltration.log | grep cat
Sep 13 20:50:09.418: vmx| USBIO:  040: f1 1c 63 61 74 20 65 73 74 61 65 73 0a
      ..cat estaes.
```

Unas líneas más abajo encontramos el contenido del archivo:

```
Sep 13 20:50:09.438: vmx| USBIO:  030: 00 e3 b7 17 00 00 01 01 08 0a 00 02 fe
86 02 8a ..............
Sep 13 20:50:09.438: vmx| USBIO:  040: b6 c7 55 53 42 73 6e 69 66 66 69 6e 67
4f 4e 34 ..USBsniffingON4
```

Previamente se observa también la ejecución del comando “pwd”, que indica el directorio actual.

La solución es entonces sha1("/root/estaes|USBsniffingON4G"):
9195d8a7543cc018ed020694fd674715b6c5821d

SSH: 2525

NMAP arroja un servicio ssh sobre el puerto 2525. Conectándose a él resulta:

```
ssh -p 2525 192.168.2.5
The authenticity of host '[192.168.2.5]:2525 ([192.168.2.5]:2525)' can't be
established.
RSA key fingerprint is 99:9c:02:d3:03:86:3a:c7:0b:b9:b3:83:f1:a1:8e:68.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.2.5]:2525' (RSA) to the list of known
hosts.
########################################
Reto, por cortesia de C.Z (@dumacx)
########################################
Usuario para ingresar: arm-reto
// ... y para subir el animo: EKO-ZSH-OK!
########################################
```

Luego ingresamos con el usuario **arm-reto,** clave **arm-reto**, y vemos en el archivo histórico .bash_history que el binario a explotar **test1** fue borrado, aparentemente por otro participante.

Flag 1

Obtenida del mensaje del día del servicio SSH: **EKO-ZSH-OK**

POP3: 5060, IMAP: 5061

Conectado al servidor POP3, y autenticando con el usuario **admin** y clave **temporal**, vemos un mail que contiene una flag:

```
To: root@localhost
Subject: Holaaaaaaaaaaaaaaaa
From: root <root@ctf.ekoparty.org>

Hola admin, te regalo esta flag: EKO-D0V-K07
----
```

A través del servicio IMAP se consigue la misma flag.

Flag 1

Obtenida del servicio POP3: **EKO-D0V-K07**

SMB: 139, 1349

Listando los recursos compartidos del servicio smb, encontramos otra flag:

```
smbclient -L ctf.ekoparty.org
Enter root's password:
Failed to load upcase.dat, will use lame ASCII-only case sensitivity rules
Failed to load lowcase.dat, will use lame ASCII-only case sensitivity rules
Anonymous login successful
Domain=[EKOPARTY] OS=[Unix] Server=[Samba 3.5.6]

Sharename         Type        Comment
---------         ----        -------
terapia           Disk        Reto por cortesia del RICTEAM (@RedInfoCol)
IPC$              IPC         IPC Service (CTF SHARE SERVER :: EKO-SH4-R3Z)

Anonymous login successful
Domain=[EKOPARTY] OS=[Unix] Server=[Samba 3.5.6]

Server            Comment
---------         -------
CTF               CTF server

Workgroup         Master
---------         -------
EKOPARTY          CTF
```

Flag 1

Obtenida de la información proporcionada por el servicio Netbios: **EKO-SH4-R3Z**

TFTP: 69

Conectamos con un cliente tftp al target, y descargamos el archivo flag.txt. Luego vemos su contenido, y obtenemos lo siguiente:

```
Ok, you got it!
Flag: EKO-HEL-LO>
Descarga: holamun.do
```

Flag 1

Obtenida del archivo flag.txt: **EKO-HEL-LO>**

Virtualhost Ekoparty: 8000

Conectando al servicio HTTP, sobre el puerto 8000, con el host virtual “ekoparty”, obtenemos otra flag:

```
<!-- Una flag mas para tomar fuerzas: EKO-NOT-RC4 -->
```

Flag 1

Obtenida del código fuente: **EKO-NOT-RC4**