

Pasos para ejecutar Ducky scripts en español con Bash Bunny

Conectar con Bash Bunny utilizando el protocolo SCP con la herramienta WinSCP



Default Settings

Username: root

Password: hak5bunny

IP Address: 172.16.64.1

DHCP Range: 172.16.64.10-12

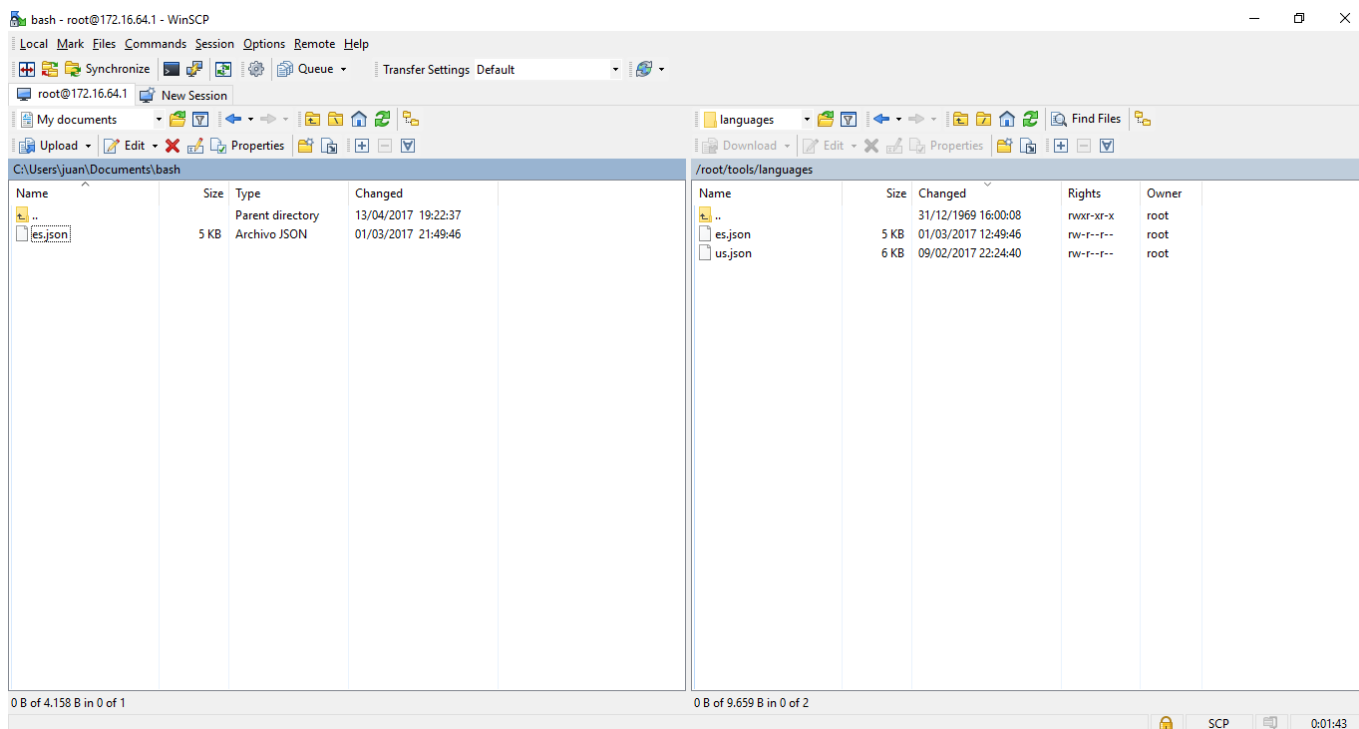


Una vez conectado con Bash Bunny copiar el fichero JSON de lenguaje español que se encuentra dentro de la carpeta (languages)

[crayon-6a9d601445a44644618120/]

a la carpeta

[crayon-6a9d601445a4a007203602/]



Dentro del fichero payload.txt hay que tener declarada la variable DUCKY_LANG='es'

```

F:\payloads\switch2\payload.txt - Notepad++
Archivo  Editar  Buscar  Vista  Configuración  Idioma  Configuración  Herramientas  Macro  Ejecutar  Plugins  Ventana  ?
ducky_script.txt  payload.txt

1  LED G
2  ATTACKMODE HID STORAGE
3
4  # Set your language here
5  LANGUAGE='es'
6  DUCKY_LANG='es'
7
8  LED R G
9  # Check for switch position to make it easier for us. (can be replaced in the future with bunny helpers)
10 check_switch()
11     switch1='cat /sys/class/gpio_sw/PA8/data'
12     switch2='cat /sys/class/gpio_sw/PL4/data'
13     switch3='cat /sys/class/gpio_sw/PL3/data'
14     echo "--- switch1 = $switch1, switch2 = $switch2, switch3 = $switch3"
15     if [ "$switch1" = "x0" ] && [ "$switch2" = "x1" ] && [ "$switch3" = "x1" ]; then
16     > SWITCH_POSITION="switch1"
17     elif [ "$switch1" = "x1" ] && [ "$switch2" = "x0" ] && [ "$switch3" = "x1" ]; then
18     > SWITCH_POSITION="switch2"
19     elif [ "$switch1" = "x1" ] && [ "$switch2" = "x1" ] && [ "$switch3" = "x0" ]; then
20     > SWITCH_POSITION="switch3"
21     else
22     > SWITCH_POSITION="invalid"
23     fi
24 }
25
26 check_switch
27
28 if [ -f "/root/udisk/payloads/${SWITCH_POSITION}/ducky_script.txt" ]; then
29     > QUACK ${SWITCH_POSITION}/ducky_script.txt
30     > LED G
31 else
32     > LED R
33     > echo "Unable to load ducky_script.txt" >> /root/debuglog.txt
34     > exit 1
35 fi
36
Normal text file  length: 1.051  lines: 36  Ln: 6  Col: 1  Sel: 0 | 0  Unix (LF)  UTF-8  INS

```

Más información

<https://github.com/hak5/bashbunny-payloads/pull/39/files>