HackTheBox – Arthropod Write Up

Tools:

- Wireshark (Kali Linux)
- tshark (Kali Linux)
- Python script to translate keystrokes (https://bitvijays.github.io/LFC-Forensics.html)

Walkthrough:

Step	Description
1	The files extracted from the zip file are "deadly_arthropod.pcap".
2	Upon inspecting the pcap file in Wireshark, There seems to be a series of "URB_ INTERRUPT" and only small changes between each packet.
3	From reading the forums, the pcap file is believed to have recorded keystrokes.
4	The next step taken was to extract each recorded keystroke from each packet with the command "tshark -r deadly_arthropod.pcap -T fields -e usb.capdata > keystrokes.txt".
5	Use the command "cat keystrokes.txt | awk 'NF' > pipe;cat pipe > keystrokes.txt".
6	After writing the data to keystrokes.txt, use the command "sed '/^$/d' keystrokes.txt > keystrokes.txt" to set it in the correct format.
7	The data inside keystrokes.txt was translated using a python script. import os,sys,operator usb_codes = {0x04:"aA", 0x05:"bB", 0x06:"cC", 0x07:"dD", 0x08:"eE", 0x09:"fF", 0x0A:"gG", 0x0B:"hH", 0x0C:"iI", 0x0D:"jJ", 0x0E:"kK", 0x0F:"lL", 0x10:"mM", 0x11:"nN", 0x12:"oO", 0x13:"pP", 0x14:"qQ", 0x15:"rR", 0x16:"sS", 0x17:"tT", 0x18:"uU", 0x19:"vV", 0x1A:"wW", 0x1B:"xX", 0x1C:"yY", 0x1D:"zZ", 0x1E:"1!", 0x1F:"2@", 0x20:"3#", 0x21:"4$", 0x22:"5%", 0x23:"6^", 0x24:"7&", 0x25:"8*", 0x26:"9(", 0x27:"0)", 0x2C:" ", 0x2D:"-_", 0x2E:"=+", 0x2F:"[{", 0x30:"]}", 0x32:"#~", 0x33:";:", 0x34:"'\"", 0x36:",<", 0x37:".>", 0x4f:">", 0x50:"<"}

	lines = ["","","","","","]
	pos = 0
	for x in open('newkeystrokes.txt','r').readlines():
	print x
	code = int(x[6:8],16)
	print code
	if code == 0:
	continue
	if code == 0x51 or code == 0x28:
	pos += 1
	continue
	if int(x[0:2],16) == 2:
	lines[pos] += usb_codes[code][1]
	else:
	lines[pos] += usb_codes[code][0]
	
	for x in lines:
	print x

8	The translated text will display text with arrows "<" and ">" eks@hackthebox.eu Th1sC0uldB3MyR3alP@ssw0rd QK<_>.<<<<H>5<<{_<I>>ck>' (Part of the final translated text is only shown as example) - The "<" represents left arrow. - The ">" represents right arrow. The final step to get the flag is to type each letter and move accordingly based on the number of arrows keys before typing the next letter to get the flag.

Flag is HTB{Please find the flag yourself ☺}