Decrypt Cryptcat stream

For do this exercise we must, at first, build a cryptcat stream and put an attacker in a strategic position so that it can sniff all the traffic between the hosts.

Hosts configuration

For this scenario our GNS3 laboratory works well, but we must only replace the switch previously configured with the **HUB** appliance provided by GNS3. This appliance will work out-of-the-box so no configuration is necessary, just the physical connection oh the hosts (Router, ubuntu hosts, raspberrypi). Here our raspberrypi hosts will work as attacker.
We use the HUB appliance so that the attacker is able to receive all data that pass through it without any other configuration.

Stream configuration

Once that the configuration is done, we can install cryptcat tool on our ubuntu hosts with this linux command:

$sudo apt update && sudo apt install cryptcat

Now we are ready to run the stream.

server side:

$cryptcat -k <<key>> -p <<port>> -l
(Example $cryptcat -k password -p 9090)

client side:

$cryptcat <<server-ip>><<server-port>> -k <<key>>
(Example $cryptcat 10.0.0.2 9090 -k password)

Attacker configuration

On attacker we need some tools, in particular we need tshark (a CLI version of wireshark) for sniff the traffic, cryptcat and netcat.
We can install it with this command:

$sudo apt install tshark cryptcat netcat

Sniff traffic

Once finished the installation of the tools and the stream between hosts has been open, we can start to sniff the data from the attacker. In particular, we are interested at TCP packets that have push flag==on and with data section.
In order to filter the traffic we can run tshark using some filters, like the ones used on wireshark.
The command that will help us is the following:

```
$sudo tshark -Y 'tcp.flags.push ==1 && data && !tcp.analysis.flags' -Tfields -e data > raw-out.txt
```

The output is saved in the file raw-out.txt.

Converting raw data to byte

Now for decrypt the stream we must convert the raw data to byte, in order to do this we will use xxd tool available on linux.

$cat raw-out.txt | xxd -r -p > crypted_data.txt

Discovering password

For discovering the password, we will perform a dictionary attacks with a wordlist, available on the course website at this link, and a tool called decryptcat.

At first we must download decryptcat and install it with the following commands:

$ git clone https://github.com/deurstijl/decryptcat.git
$cd decryptcat/
$make linux

Now we are ready to discover the password:

$./decryptcat crypted_data.txt wordlist

If the tools is able to discover the password, it will print it at the end of the execution.

Decrypt the stream

For decrypting the stream we will use a simple trick, on the attacker we open a stream on two different terminals.
In one terminal, we must run a cryptcat in listen mode, giving as key the one discovered before. Here cryptcat will decrypt the data and show in plain text the result.
In the other terminal, we must open a netcat client that will send the encrypted data as is.

On server side:

$cryptcat -k <<key>> -l -p 9090

On Client side:

$nc -w 1 127.0.0.1 9090 < crypted_data.txt