DC3
Cyber Training Academy

SCAPY QUICK TIPS

WHAT IS IT?

SCAPY is a Python-based tool for interactive packet manipulation

WHAT CAN IT DO?

Forge or decode packets, send and capture packets, match requests and replies; perform scanning, tracerouting, probing, unit tests, attacks, network discovery, and more

GETTING HELP

```
>>> help(ls)
```

CRAFTING & VIEWING PACKETS

Create a Packet

```
>>> i=IP()
>>> i.src="192.168.229.55"
>>> i.dst="192.168.229.13"
>>> icmp=ICMP()
>>> icmp.type=8
>>> icmp.code=0
```

In this example, the created packet has:

- An IP header containing the source IP 192.168.229.55
- A Destination IP of 192.168.229.13
- An ICMP Header of type 8 and code 0

Combining Layers

Scapy uses layers, which are individual functions that can be linked using the “/” character

```
>>> packet=i/icmp
```

Viewing a Summary of the Packet

```
>>> packet.summary()
```

Viewing the Contents of the Packet

```
>>> packet.show()
```

SENDING & RECEIVING PACKETS

Sending a Packet Without a Custom Ether Layer

```
>>> send(packet)
.
Sent 1 packets.
```

Alternatively, you could use:

```
>>> send(IP(src="192.168.229.55",
dst="192.168.229.13")/ICMP(type=8,
code=0))
.
Sent 1 packets.
```

For more info, visit:
https://scapy.readthedocs.io/en/latest/

Sending and Receiving Functions

sr(): sends packets and receives answers; returns a couple of packets that have answers, as well as unanswered packets

sr1(): returns only one packet which answered the sent packet sent

```
>>> sr1(IP(src="192.168.229.13")/
ICMP()/"Hello World")
Begin emission:
Finished sending 1 packets.
*
Received 2 packets, got 1 answers,
remaining 0 packets
<IP version=4 ihl=5 tos=0x0 len=39
id=102 flags= frag=0 ttl=128 proto
=icmp chksum=0xeef3 src=192.168.229
.13 dst=192.168.229.29 options=[] |
<ICMP type=echo-reply code=0 chksum
=0xae31 id=0x0 seq=0x0 | <Raw load
='Hello World' |<Padding load
='\x00\x00\x00\x00\x00\x00\x00' |>>>>
```

srp(): sends packets and receives answers for layer 2 or ethernet packets