

Re: mystery martian source from 127.0.0.1 – more details

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-12/msg00242.html>

- *From:* Tauno Voipio <tauno.voipio@xxxxxxxxxxxxxx>
 - *Date:* Thu, 08 Dec 2005 22:26:12 GMT
-

EricT wrote:

```
Frame 1 (60 bytes on wire, 60 bytes captured)
  Arrival Time: Dec  8, 2005 22:33:57.-11226009
  Time delta from previous packet: 0.000000000 seconds
  Time since reference or first frame: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 60 bytes
  Capture Length: 60 bytes
  Protocols in frame: eth:ip:tcp
```

This is OK.

```
Ethernet II, Src: Cisco_8d:98:70 (00:09:7b:8d:98:70), Dst: 3com_48:2c:65
(00:01:03:48:2c:65)
  Destination: 3com_48:2c:65 (00:01:03:48:2c:65)
  Source: Cisco_8d:98:70 (00:09:7b:8d:98:70)
  Type: IP (0x0800)
  Trailer: 000000000000
```

The packet comes from your DSL box to the computer,
but claims to be from local host. The Ethernet
addresses can be trusted here, everything else
seems to be fake.

```
Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 80.219.238.182
(80.219.238.182)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 40
  Identification: 0x25b1 (9649)
  Flags: 0x00
    0... = Reserved bit: Not set
```

Re: mystery martian source from 127.0.0.1 – more details

```
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 126
Protocol: TCP (0x06)
Header checksum: 0x5d81 [correct]
  Good: True
  Bad : False
Source: 127.0.0.1 (127.0.0.1)
Destination: 80.219.238.182 (80.219.238.182)
Transmission Control Protocol, Src Port: http (80), Dst Port:
eicon-server (1438), Seq: 0, Ack: 0, Len: 0
  Source port: http (80)
  Destination port: eicon-server (1438)
  Sequence number: 0      (relative sequence number)
  Acknowledgement number: 0    (relative ack number)
  Header length: 20 bytes
  Flags: 0x0014 (RST, ACK)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .1.. = Reset: Set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 0
Checksum: 0x796e [correct]
```

This claims to be a reset packet for a non-existing connection.

IIRC, there is a port scanning tool in circulation which probes the targets with non-existent resets, but AFAIK, it works only in the local network due to the fake sender IP.

It may be looking for a Web server to crack or maybe for p2p traffic piggy-backed on a Web request.

Check for any open ports
with:

```
netstat -tupan
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
```

Re: mystery martian source from 127.0.0.1 – more details

```
State      PID/Program name
tcp        0      0 0.0.0.0:32769      0.0.0.0:*
LISTEN    -
tcp        0      0 0.0.0.0:111        0.0.0.0:*
LISTEN    6436/portmap
tcp        0      0 127.0.0.1:948      0.0.0.0:*
LISTEN    7556/fam
tcp        0      0 :::22              :::*
LISTEN    7074/sshd
udp        0      0 0.0.0.0:1042      0.0.0.0:*
-
udp        0      0 0.0.0.0:68         0.0.0.0:*
6211/dhcpd
udp        0      0 0.0.0.0:111        0.0.0.0:*
6436/portmap
udp        0      0 192.168.200.1:123  0.0.0.0:*
7004/ntpd
udp        0      0 80.219.238.182:123 0.0.0.0:*
7004/ntpd
udp        0      0 192.168.100.10:123 0.0.0.0:*
7004/ntpd
udp        0      0 127.0.0.1:123     0.0.0.0:*
7004/ntpd
udp        0      0 0.0.0.0:123       0.0.0.0:*
7004/ntpd
udp        0      0 :::123            :::*
7004/ntpd
```

However, all NEW connections of any protocol to the firewall from outside are dropped.

This is OK - seems clean.

In principle, the kernel considers a packet martian if its source address is obviously incorrect for the interface it's coming in.

I thought so, that is why i want to know what is going on in this case.

See above.

It seems to me that your firewall and the martian trap

Re: mystery martian source from 127.0.0.1 – more details

have done their job and the attackers are failing.

HTH

Best regards from Helsinki, the home city of Linux!

--

Tauno Voipio
tauno voipio (at) iki fi

.