

Help Interpreting data from Wireshark

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2007-02/msg00012.html>

- *From:* DaveM <dave@xxxxxxxxxxx>
 - *Date:* Sun, 04 Feb 2007 21:21:00 GMT
-

Hello,

Today while on the Internet I got the following data from p54A05FE2.dip.t-dialin.net on my Wireshark display. A quick search on Google indicates a spammer. Can someone help me interpret this data and recommend a security posture to mitigate?

What concerns me is that the packet seemed to have a source address of 192.168.1.1 but later in the packet you see the dest as 84.160.95.226

How do I know if they actually logged onto my machine? I searched /var/log but found nothing.

I only listed one packet for the example but got a boat load on my screen. Data follows:

```
No. Time Source Destination Protocol Info
4913 2007-02-04 15:48:00.462669 p54A05FE2.dip.t-dialin.net DENVER.local ICMP Destination
unreachable (Port unreachable)
```

```
Frame 4913 (134 bytes on wire, 134 bytes captured)
Arrival Time: Feb 4, 2007 15:48:00.462669000
[Time delta from previous packet: 0.024400000 seconds]
[Time since reference or first frame: 22444.768518000 seconds]
Frame Number: 4913
Packet Length: 134 bytes
Capture Length: 134 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:udp:rtp]
[Coloring Rule Name: ICMP errors]
[Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 11 || icmp.type eq 5]
Ethernet II, Src: 192.168.1.1 (00:03:c9:5b:40:0f), Dst: DENVER.local (00:0e:2e:99:72:ee)
Destination: DENVER.local (00:0e:2e:99:72:ee)
Address: DENVER.local (00:0e:2e:99:72:ee)
....0 .... = IG bit: Individual address (unicast)
....0. .... = LG bit: Globally unique address (factory default)
Source: 192.168.1.1 (00:03:c9:5b:40:0f)
Address: 192.168.1.1 (00:03:c9:5b:40:0f)
....0 .... = IG bit: Individual address (unicast)
....0. .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
```

Help Interpreting data from Wireshark

Internet Protocol, Src: p54A05FE2.dip.t-dialin.net (84.160.95.226), Dst: DENVER.local (192.168.2.101)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0xd0 (DSCP 0x34: Unknown DSCP; ECN: 0x00)
1101 00.. = Differentiated Services Codepoint: Unknown (0x34)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 120
Identification: 0xca34 (51764)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0x78f0 [correct]
[Good: True]
[Bad : False]
Source: p54A05FE2.dip.t-dialin.net (84.160.95.226)
Destination: DENVER.local (192.168.2.101)
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0x74e6 [correct]
Internet Protocol, Src: DENVER.local (192.168.2.101), Dst: p54A05FE2.dip.t-dialin.net (84.160.95.226)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 92
Identification: 0x0000 (0)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xc2f1 [correct]
[Good: True]
[Bad : False]
Source: DENVER.local (192.168.2.101)
Destination: p54A05FE2.dip.t-dialin.net (84.160.95.226)
User Datagram Protocol, Src Port: rfe (5002), Dst Port: 5010 (5010)
Source port: rfe (5002)
Destination port: 5010 (5010)
Length: 72
Checksum: 0x3d33 [correct]

Help Interpreting data from Wireshark

[Good Checksum: True]
[Bad Checksum: False]
Real-Time Transport Protocol
[Stream setup by SDP (frame 4902)]
[Setup frame: 4902]
[Setup Method: SDP]
10.. = Version: RFC 1889 Version (2)
..0. = Padding: False
...0 = Extension: False
.... 0000 = Contributing source identifiers count: 0
0... = Marker: False
Payload type: SPEEX (114)
Sequence number: 1078
Timestamp: 320
Synchronization Source identifier: 3414068057
Payload: 2DC25016610045576CD00FFFF401E73F2EF1B7B19BEFC6E9...

Best regards,

Dave

--

Dave McCarthy
RLU #415791