

SANS Christmas Challenge

Player: C.S.Lee
Email: geek001[at]gmail[dot]com
Date: 20071227

The Starter

```
shell>tshark -c 2 -t ad -xnr xmas_Starter.pcap | egrep '^ 2' -A 100
 2 2007-12-24 12:47:42.798056 192.168.25.100 -> 192.168.25.128 TCP 7337 > 1000
[SYN] Seq=0 Len=200
```

```
0000 00 0c 29 53 62 bd 00 0c 29 5c aa a2 08 00 45 00    ..)Sb...)\....E.
0010 00 f0 87 b3 00 00 40 06 3e 20 c0 a8 19 64 c0 a8    .....@.> ....d..
0020 19 80 1c a9 03 e8 46 3d a8 c0 02 f5 7e 62 50 02    .....F=....~bP.
0030 02 00 43 33 00 00 53 57 34 67 64 47 68 6c 49 47    ..C3..SW4gdGh1IG
0040 31 76 64 6d 6c 6c 49 45 45 67 51 32 68 79 61 58    1vdm1lIEEgQ2hyaX
0050 4e 30 62 57 46 7a 49 45 4e 68 63 6d 39 73 4c 43    N0bWFzIENhcm9sLC
0060 42 6f 62 33 63 67 62 57 46 75 65 53 42 75 61 57    Bob3cgbWFueSBuaW
0070 64 6f 64 43 68 7a 4b 53 42 6b 61 57 51 67 64 47    dodChzKSBkaWQgdG
0080 68 6c 49 48 52 6f 63 6d 56 6c 49 48 4e 77 61 58    h1IHRocmVlIHNwaX
0090 4a 70 64 48 4d 67 59 32 39 74 5a 53 42 30 62 79    JpdHMgY29tZSB0by
00a0 42 32 61 58 4e 70 64 44 38 3d 00 00 00 00 00 00    B2aXNpdD8=.....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
```

It should be base64, look at the padding = to ensure multiple of 4 bytes, python is here to stay -

```
shell>printf \
"SW4gdGh1IG1vdm1lIEEgQ2hyaXN0bWFzIENhcm9sLCBob3cgbWFueSBuaWdodChzKSBkaWQgdGh1IHRocm
VlIHNwaXJpdHMgY29tZSB0byB2aXNpdD8=" | \
python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
In the movie A Christmas Carol, how many night(s) did the three spirits come to
visit?
```

This leads to first packet because only one night.

The Challenge

```
shell>printf "QWxsIEkgd2FudCBmb3IgcQ2hyaXN0bWFzIGlzlG15IF9fX18gRnJvbnQgVGvldGgu" | \
python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
All I want for Christmas is my ____ Front Teeth.
```

This leads to second packet because two front teeth.

```
shell>printf \
"SG93IG1hbknkgcmVpbmRlZXIgaGF2ZSBuYW11cyB0aGF0IGJlZ2luIHdpdGggdGh1IGxldHRlciAi.RCI/"
| python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
How many reindeer have names that begin with the letter "D"?
```

The answer is 3 : Dasher, Donder, Dancer

```
shell>printf "SG93IG1hbknkgcmVpbmRlZXIgcHVsbCBTYW50YSdzIHNSZWlnaD8=" | \
python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
```

How many reindeer pull Santa's sleigh?

The answer is 9: Rudolph, Dasher, Dancer, Prancer, Vixen, Donner, Blitzen, Cupid and Comet

```
shell>printf "SG93IG1hbnkgcG1wZXJzIHBPcGluZyBkaWQgbXkgdHJlZSBsb3ZlIGdpdmUgdG8gbWU/"
| python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
How many pipers piping did my true love give to me?
```

The answer is 11

```
shell>printf \
"SG93IG1hbnkgZGF5cyBpbjB0aGUgc29uZyB0aGUgX19fIERheXMgb2YgQ2hyaXN0bWFzPw==" | \
python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
How many days in the song the ___ Days of Christmas?
```

The answer is 12

```
shell>printf \
"T2YgdGhlIDM2NSBkYXlzlIGluIHllYXIsIHdoYXQgbnVtYmVyIGlzIENocmlzdG1hcyBEYXk/IA==" | \
python -c "import base64,sys; base64.decode(sys.stdin,sys.stdout)"
Of the 365 days in year, what number is Christmas Day?
```

For leap year it is 365-5 and normal year 365-6(it states 365 days in year) so the answer should be 359

Anyway my first guess is this is url encoding(blame %20) but it doesn't seem right, and I notice the crazy tcp flags here -

```
shell>tcpdump -vtttttnnr xmas_challenge_2007.pcap tcp[13]=0x7F
shell>tshark -t ad -nr xmas_challenge_2007.pcap -R 'tcp.flags==0x7F'
```

One thing funny is that the last packet that seen with this odd tcp flags(FIN, SYN, RST, PSH, ACK, URG, ECN) is the 365th packet, wondering if this is coincident or SANS nuts purposely do it. I also notice this -

```
2007-11-04 13:22:51.836149 IP (tos 0x0, ttl 64, id 61620, offset 0, flags [none],
proto TCP (6), length 140) 192.168.25.100.7337 > 192.168.25.128.1000: SFRPE, cksum
0x942f (correct), 1051609149:1051609249(100) ack 1942617868 win 512 urg 0 [RST+
87%20101%20NULL%20119%20105%20]
0x0000: 000c 2953 62bd 000c 295c aaa2 0800 4500 ..)Sb...)\....E.
0x0010: 008c f0b4 0000 4006 d582 c0a8 1964 c0a8 .....@.....d..
0x0020: 1980 1ca9 03e8 3eae 483d 73c9 ff0c 507f .....>.H=s...P.
0x0030: 0200 942f 0000 3837 2532 3031 3031 2532 .../.87%20101%2
0x0040: 304e 554c 4c25 3230 3131 3925 3230 3130 0NULL%20119%2010
0x0050: 3525 3230 3131 3525 3230 3130 3425 3230 5%20115%20104%20
0x0060: 4e55 4c4c 2532 3031 3231 2532 3031 3131 NULL%20121%20111
0x0070: 2532 3031 3137 2532 304e 554c 4c25 3230 %20117%20NULL%20
0x0080: 3937 2532 304e 554c 4c25 3230 3737 2532 97%20NULL%2077%2
0x0090: 3031 3031 2532 3031 3134 0101%20114
```

Anyway my first guess is this is url encoding(blame %20) but it doesn't seem right. However the [RST+ 87%20101%20NULL%20119%20105%20] raises my interest. Googling renders this interesting result -

<http://www.ethereal.com/lists/ethereal-users/200404/msg00203.html>

A TCP SHOULD allow a received RST segment to include data.

DISCUSSION

It has been suggested that a RST segment could contain **ASCII text** that encoded and explained the cause of the RST. No standard has yet been established for such data.

After the reading I suspect it can be decoded with "man ascii" -

```
87 101 119 105 115 104 121 111 117 97 77 101 114 114 121 67 104 114 105 115 116 109
97 115 44 0D 0A(\r\n)
87 101 119 105 115 104 121 111 117 97 77 101 114 114 121 67 194 114 195 115 116 198
97 115 44 0D 0A(\r\n)
87 101 119 105 115 104 121 111 117 97 77 101 114 114 121 67 194 114 195 115 116 198
97 115 44 0D 0A(\r\n)
97 110 100 97 72 97 112 112 121 78 101 119 89 101 97 114 33 33 33
```

Note: The 20 is hex which is space that i didn't put in here to make it look cleaner. Damn unicode and NULL! I think it should have message - echo 'SANS Incident Handlers' > /dev/null'.

I'm using this since I'm lazy - <http://www.fourmilab.ch/webtools/unum/>

```
shell>unum.pl 87 101 119 105 115 104 121 111 117 97 77 101 114 114 121 67 104 114
105 115 116 109 97 115 44 | \
awk '{ print $5 }'
```

```
We wish you a Merry Christmas,
We wish you a Merry Christmas,
We wish you a Merry Christmas,
and a Happy New Year !!!
```

To SANS Incident Handlers(especially finchy), this is not message, this is song!

Some of misleading but fun part

I try to locate packets with tcp reset flags set using tshark -

```
shell>tshark -t ad -nr xmas_challenge_2007.pcap -R 'tcp.flags.reset==1'
```

It leads to interesting packets too -

```
shell>tcpdump -tttttnnr xmas_challenge_2007.pcap tcp[13]=0x0F
```

```
shell>tshark -t ad -nr xmas_challenge_2007.pcap -R 'tcp.flags == 0x0F'
333 2007-11-04 13:20:06.353094 192.168.25.100 -> 192.168.25.128 TCP [TCP
Retransmission] 7337 > 1000 [FIN, SYN, RST, PSH] Seq=4072480441 Len=100
334 2007-11-04 13:20:07.350474 192.168.25.100 -> 192.168.25.128 TCP [TCP
Retransmission] 7337 > 1000 [FIN, SYN, RST, PSH] Seq=2798099836 Len=100
335 2007-11-04 13:20:08.350536 192.168.25.100 -> 192.168.25.128 TCP [TCP
Retransmission] 7337 > 1000 [FIN, SYN, RST, PSH] Seq=2715696440 Len=100
336 2007-11-04 13:20:09.350496 192.168.25.100 -> 192.168.25.128 TCP [TCP
Retransmission] 7337 > 1000 [FIN, SYN, RST, PSH] Seq=3520054726 Len=100
Truncated Output ....
```

That's exactly 12 packets and SANS plans to give me christmas gifts through out 12 days?

