

Alert Event Analysis

Event Snort-TCP_Attempted_Information_Leak
Category Scanning
Description SOC have detected suspicious network scanning on xxx network
Date / Time Start : Sunday 09 March 2008 16:11:47 +0800
End : Sunday 09 March 2008 17:52:26 +0800
Source IP a1.a2.a3.a4
Destination IP b1.b2.b3.b4
Signatures Detected BLEEDING-EDGE SCAN NMAP -sA (1)
Number of Event 250

Sample Raw Log :

```
<158>snort: [1:2000538:4] BLEEDING-EDGE SCAN NMAP -sA (1) [Classification: Attempted Information Leak] [Priority: 2]: {TCP} a1.a2.a3.a4:80 -> b1.b2.b3.b4:15086
```

The rules that detect this scanning signature : BLEEDING-EDGE SCAN NMAP -sA (1) or the latest one called : ET SCAN NMAP -sA (1) where ET stands for Emerging Threats.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sA (1)"; fragbits: !D; dsize: 0; flags: A,12; window: 1024; reference:arachnids,162; classtype: attempted-recon; sid: 2000538; rev:5;)
```

Rule Description:

The rule is based on non-payload detection method.

For IP Layer, the main signature for the alert to be triggered is based on the Fragmentation and reserved Bit in the IP header. In this case only Don't Fragment Bit enabled packet will be ignored.

```
fragbits: !D
```

While the payload size of the packet must be zero

```
dsize: 0
```

For TCP Layer, the main signature will be on the control flag and the window size. Only packet with the Acknowledge (ACK) option enabled and with the window size of 1024 Bytes

```
flags: A,12; window: 1024
```

So the question is whether the source IP really performing nmap ACK scanning or not. Let us consider few scenarios.

SCENARIO 1

A. Source IP (a1.a2.a3.a4) really performing nmap ACK scanning from port 80.

First of all we need to simulate the scanning activity to get the clear picture

In this simulation, 192.168.4.20 will be the attacker while 192.168.4.127 will be the target. To simulate the events reported, we will execute nmap -sA with source port 80 from 192.168.4.20 to 192.168.4.127.

```
ayoi# nmap -sA --source-port 80 192.168.4.127
Starting Nmap 4.20 ( http://insecure.org ) at 2008-03-10 14:46 MYT
```

Below is the session data generated by the activity

```
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.80: . ack 1718529464 win 2048
13:59:00.892083 IP 192.168.4.20.80 > 192.168.4.127.53: . ack 1817132945 win 3072
13:59:01.992738 IP 192.168.4.20.80 > 192.168.4.127.53: . ack 3666296980 win 1024
13:59:01.993247 IP 192.168.4.20.80 > 192.168.4.127.80: . ack 3322425882 win 3072
13:59:01.993654 IP 192.168.4.20.80 > 192.168.4.127.554: . ack 3954598287 win 1024
13:59:01.994093 IP 192.168.4.20.80 > 192.168.4.127.389: . ack 1397273947 win 4096
13:59:01.994193 IP 192.168.4.20.80 > 192.168.4.127.256: . ack 3032925021 win 1024
13:59:01.994658 IP 192.168.4.20.80 > 192.168.4.127.443: . ack 3616913710 win 3072
13:59:01.995096 IP 192.168.4.20.80 > 192.168.4.127.21: . ack 3566764576 win 3072
```

And now let see whether this traffic will trigger the same alert with the one detected by the SOC.

```
ayoi# snort -c /usr/NSM/etc/snort.conf -r 2008-03-10-13:58.nmap_sA_source80.pcap -l .
```

```
-----SNIP-----
```

```
Snort processed 1662 packets.
```

```
Breakdown by protocol:
```

```
TCP: 1656 (99.639%)
```

```
UDP: 3 (0.181%)
```

```
ICMP: 3 (0.181%)
```

```
ARP: 0 (0.000%)
```

```
EAPOL: 0 (0.000%)
```

```
IPv6: 0 (0.000%)
```

```
ETHLOOP: 0 (0.000%)
```

```
IPX: 0 (0.000%)
```

```
FRAG: 0 (0.000%)
```

```
OTHER: 0 (0.000%)
```

```
DISCARD: 0 (0.000%)
```

```
InvChkSum: 0 (0.000%)
```

```
Action Stats:
```

```
ALERTS: 820
```

```
LOGGED: 820
```

```
PASSED: 0
```

```
Snort exiting
```

For the nmap activity, it does generate 820 alerts. Let us see what kind of alert generated.

```
ayoi# less alert
[**] [1:2000538:5] ET SCAN NMAP -sA (1) [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/10-13:59:00.891305 192.168.4.20:80 -> 192.168.4.127:1723
TCP TTL:40 TOS:0x0 ID:2394 IpLen:20 DgmLen:40
***A**** Seq: 0x11BBA413 Ack: 0x7BCC7674 Win: 0x400 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS162]

[**] [1:2000538:5] ET SCAN NMAP -sA (1) [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/10-13:59:00.891305 192.168.4.20:80 -> 192.168.4.127:21
TCP TTL:56 TOS:0x0 ID:44481 IpLen:20 DgmLen:40
***A**** Seq: 0x11BBA413 Ack: 0x2C74F92B Win: 0x400 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS162]
```

Perhaps we should examine the main reason for that kind of alerts to be triggered by looking at the nmap traffics IP and TCP Headers

```
ayoi# tcpdump -Xlnnr 2008-03-10-13:58.nmap_sA_source80.pcap | less

13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.3389: . ack 773023477 win 1024
0x0000: 4500 0028 3bab 0000 3406 c141 c0a8 0414      E..(;...4..A....
0x0010: c0a8 047f 0050 0d3d 11bb a413 2e13 66f5 ..... P.=.....f.
0x0020: 5010 0400 c98c 0000          P.....

13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.1723: . ack 2076997236 win 1024
0x0000: 4500 0028 095a 0000 2806 ff92 c0a8 0414      E..(.Z..(.....
0x0010: c0a8 047f 0050 06bb 11bb a413 7bcc 7674 .....P.....{.vt
0x0020: 5010 0400 72d6 0000          P...r...

13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.21: . ack 745863467 win 1024
0x0000: 4500 0028 adc1 0000 3806 4b2b c0a8 0414      E..(....8.K+....
0x0010: c0a8 047f 0050 0015 11bb a413 2c74 f92b .....P.....,t.+
0x0020: 5010 0400 461d 0000          P...F...
```

When we examine the packet we can see that the Fragmentation Bit was not set in those packets and also that the window size of the packet = 1024 Bytes (0000 (italic) and 0400 (bold) in hex format)

SCENARIO 2

And now let proceed with scenario 2

The source IP (a1.a2.a3.a4) actually being scanned by the destination IP (b1.b2.b3.b4)

In this simulation we will use 192.168.4.20 as source performing nmap -sA scanning to 192.168.4.127 at port 80

```
ayoi# nmap -sA 192.168.4.127 -p 80
Starting Nmap 4.20 ( http://insecure.org ) at 2008-03-10 16:08 MYT
```

Below is the traffic generated by this activity.

```
14:00:45.310717 IP 192.168.4.20.48777 > 192.168.4.127.80: . ack 400921770 win 1024
14:00:45.311220 IP 192.168.4.127.80 > 192.168.4.20.48777: R 400921770:400921770(0) win 0
14:00:45.412238 IP 192.168.4.20.48778 > 192.168.4.127.80: . ack 1635987751 win 2048
14:00:45.412776 IP 192.168.4.127.80 > 192.168.4.20.48778: R 1635987751:1635987751(0) win 0
```

Let see what kind of alert generated from this traffic

```
ayoi# snort -c /usr/NSM/etc/snort.conf -r 2008-03-10-14:00.nmap_sA_dest80.pcap -l .
```

Snort processed 10 packets.

=====
Breakdown by protocol:

TCP: 4 (40.000%)
UDP: 3 (30.000%)
ICMP: 3 (30.000%)
ARP: 0 (0.000%)
EAPOL: 0 (0.000%)
IPv6: 0 (0.000%)
ETHLOOP: 0 (0.000%)
IPX: 0 (0.000%)
FRAG: 0 (0.000%)
OTHER: 0 (0.000%)
DISCARD: 0 (0.000%)
InvChkSum: 0 (0.000%)
=====

Action Stats:

ALERTS: 1
LOGGED: 1
PASSED: 0
=====

For this kind of traffic its only generate one alert which is

```
[**] [1:2000538:5] ET SCAN NMAP -sA (1) [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/10-14:00:45.310717 192.168.4.20:48777 -> 192.168.4.127:80
TCP TTL:52 TOS:0x0 ID:50674 IpLen:20 DgmLen:40
***A**** Seq: 0x21A1FD15 Ack: 0x17E594AA Win: 0x400 TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS162]
```

Based on the events detected by the SOC, the amount of events occurred is around 250 events which at least eliminate the possibility that b1.b2.b3.b4 is performing nmap scanning to a1.a2.a3.a4 port 80.

If we study the purpose of performing `-sA` (TCP ACK scanning), as stated in the nmap manual;

`-sA` (TCP ACK scan)

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

The ACK scan probe packet has only the ACK flag set (unless you use `--scanflags`). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 1, 2, 3, 9, 10, or 13), are labeled filtered.

Also we can eliminate the possibility of normal web browsing due to the size of “window Size Option” where usually for normal traffic transaction, system will try to allocate the maximum size of buffer available (65KB) for sufficient data transfer (Refer traffic below)

```
16:50:57.338836 IP 192.168.4.127.3115 > 61.8.212.114.80: S 1670549916:1670549916(0) win 65535 <mss 1460,nop,nop,sackOK>
0x0000: 4500 0030 920e 4000 8006 9217 c0a8 047f E..0..@.....
0x0010: 3d08 d472 0c2b 0050 6392 919c 0000 0000 =.r.+Pc.....
0x0020: 7002 ffff aad3 0000 0204 05b4 0101 0402 p.....
```

```
16:50:57.360217 IP 61.8.212.114.80 > 192.168.4.127.3115: S 1107226506:1107226506(0) ack 1670549917 win 6144 <mss 1460,sackOK,nop,nop>
0x0000: 4500 0030 d0a2 4000 7306 6083 3d08 d472 E..0..@.s`.=.r
0x0010: c0a8 047f 0050 0c2b 41fe ef8a 6392 919d .....P.+A...c...
0x0020: 7012 1800 6139 0000 0204 05b4 0402 0101 p...a9.....
```

```
16:50:57.360275 IP 192.168.4.127.3115 > 61.8.212.114.80: . ack 1 win 65535
0x0000: 4500 0028 920f 4000 8006 921e c0a8 047f E..(..@.....
0x0010: 3d08 d472 0c2b 0050 6392 919d 41fe ef8b =.r.+Pc...A...
0x0020: 5010 ffff a5fd 0000 P.....
```

```
16:50:57.360407 IP 192.168.4.127.3115 > 61.8.212.114.80: P 1:497(496) ack 1 win 65535
0x0000: 4500 0218 9210 4000 8006 902d c0a8 047f E.....@....-....
0x0010: 3d08 d472 0c2b 0050 6392 919d 41fe ef8b =.r.+Pc...A...
0x0020: 5018 ffff 2fe6 0000 4745 5420 2f63 6865 P.../...GET./che
0x0030: 636b 5f75 726c 2f68 7474 703a 2f2f 7777 ck_url/http://ww
0x0040: 772e 676f 6f67 6c65 2e63 6f6d 2e6d 792f w.google.com.my/
0x0050: 3132 12
```

Also it seems that the source IP is using dynamic IP implementation which somehow reduced the possibility of having a web server or web page on its machine. And even now it seems that the IP has been released from the machine perhaps due to the expiry of DHCP lease period or communication termination.

TRACE 1 : 2008-03-10-13:58.nmap_sA_source80.pcap

```
13:59:00.890700 IP 192.168.4.20.80 > 192.168.4.127.113: . ack 227865554 win 4096
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.3389: . ack 773023477 win 1024
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.1723: . ack 2076997236 win 1024
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.21: . ack 745863467 win 1024
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.443: . ack 865242330 win 2048
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.256: . ack 1516066473 win 1024
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.389: . ack 635740056 win 3072
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.554: . ack 1151977367 win 2048
13:59:00.891305 IP 192.168.4.20.80 > 192.168.4.127.80: . ack 1718529464 win 2048
13:59:00.892083 IP 192.168.4.20.80 > 192.168.4.127.53: . ack 1817132945 win 3072
13:59:01.992738 IP 192.168.4.20.80 > 192.168.4.127.53: . ack 3666296980 win 1024
13:59:01.993247 IP 192.168.4.20.80 > 192.168.4.127.80: . ack 3322425882 win 3072
13:59:01.993654 IP 192.168.4.20.80 > 192.168.4.127.554: . ack 3954598287 win 1024
13:59:01.994093 IP 192.168.4.20.80 > 192.168.4.127.389: . ack 1397273947 win 4096
13:59:01.994193 IP 192.168.4.20.80 > 192.168.4.127.256: . ack 3032925021 win 1024
13:59:01.994658 IP 192.168.4.20.80 > 192.168.4.127.443: . ack 3616913710 win 3072
13:59:01.995096 IP 192.168.4.20.80 > 192.168.4.127.21: . ack 3566764576 win 3072
13:59:01.995199 IP 192.168.4.20.80 > 192.168.4.127.1723: . ack 2689384797 win 4096
13:59:01.995631 IP 192.168.4.20.80 > 192.168.4.127.3389: . ack 227270693 win 2048
13:59:01.995741 IP 192.168.4.20.80 > 192.168.4.127.113: . ack 1214244114 win 3072
13:59:02.095208 IP 192.168.4.20.80 > 192.168.4.127.25: . ack 1840518078 win 1024
13:59:02.095635 IP 192.168.4.20.80 > 192.168.4.127.636: . ack 1232885558 win 4096
13:59:02.095735 IP 192.168.4.20.80 > 192.168.4.127.23: . ack 37863403 win 3072
13:59:02.096162 IP 192.168.4.20.80 > 192.168.4.127.1384: . ack 715054709 win 1024
13:59:02.099703 IP 192.168.4.20.80 > 192.168.4.127.1031: . ack 606005551 win 3072
13:59:02.100214 IP 192.168.4.20.80 > 192.168.4.127.1523: . ack 1767841583 win 3072
13:59:02.100634 IP 192.168.4.20.80 > 192.168.4.127.895: . ack 1677229236 win 4096
13:59:02.100734 IP 192.168.4.20.80 > 192.168.4.127.1388: . ack 1321418930 win 1024
13:59:02.101180 IP 192.168.4.20.80 > 192.168.4.127.86: . ack 1959562883 win 3072
13:59:02.196702 IP 192.168.4.20.80 > 192.168.4.127.1384: . ack 4144076777 win 1024
13:59:02.197207 IP 192.168.4.20.80 > 192.168.4.127.23: . ack 729359616 win 2048
13:59:02.197636 IP 192.168.4.20.80 > 192.168.4.127.636: . ack 4287528677 win 4096
13:59:02.197735 IP 192.168.4.20.80 > 192.168.4.127.25: . ack 4172961455 win 4096
13:59:02.201692 IP 192.168.4.20.80 > 192.168.4.127.86: . ack 3238221372 win 2048
13:59:02.202198 IP 192.168.4.20.80 > 192.168.4.127.1388: . ack 351228122 win 2048
13:59:02.202631 IP 192.168.4.20.80 > 192.168.4.127.895: . ack 4235784988 win 3072
13:59:02.202730 IP 192.168.4.20.80 > 192.168.4.127.1523: . ack 3456405842 win 3072
13:59:02.203163 IP 192.168.4.20.80 > 192.168.4.127.1031: . ack 1304024762 win 4096
13:59:02.230334 IP 192.168.4.20 > 192.168.4.127: ICMP 192.168.4.20 udp port 137 unreachable, length 36
13:59:02.298702 IP 192.168.4.20.80 > 192.168.4.127.2009: . ack 1293898428 win 2048
13:59:02.299189 IP 192.168.4.20.80 > 192.168.4.127.4125: . ack 1131469874 win 2048
13:59:02.299631 IP 192.168.4.20.80 > 192.168.4.127.424: . ack 646478133 win 2048
13:59:02.299731 IP 192.168.4.20.80 > 192.168.4.127.18181: . ack 1238211158 win 1024
13:59:02.300166 IP 192.168.4.20.80 > 192.168.4.127.679: . ack 1498393076 win 3072
13:59:02.303342 IP 192.168.4.20.80 > 192.168.4.127.375: . ack 2099183610 win 1024
13:59:02.303342 IP 192.168.4.20.80 > 192.168.4.127.880: . ack 2117580354 win 2048
13:59:02.303342 IP 192.168.4.20.80 > 192.168.4.127.754: . ack 2074011594 win 4096
13:59:02.303342 IP 192.168.4.20.80 > 192.168.4.127.783: . ack 2105785901 win 2048
13:59:02.303342 IP 192.168.4.20.80 > 192.168.4.127.3: . ack 1413135547 win 3072
13:59:02.399705 IP 192.168.4.20.80 > 192.168.4.127.4125: . ack 416016383 win 1024
13:59:02.400213 IP 192.168.4.20.80 > 192.168.4.127.2009: . ack 3428124644 win 3072
13:59:02.403690 IP 192.168.4.20.80 > 192.168.4.127.3: . ack 3517893901 win 3072
13:59:02.404260 IP 192.168.4.20.80 > 192.168.4.127.783: . ack 2312158487 win 2048
13:59:02.404705 IP 192.168.4.20.80 > 192.168.4.127.754: . ack 3217655726 win 2048
13:59:02.405117 IP 192.168.4.20.80 > 192.168.4.127.880: . ack 3342226904 win 4096
13:59:02.405217 IP 192.168.4.20.80 > 192.168.4.127.375: . ack 320082162 win 3072
13:59:02.405614 IP 192.168.4.20.80 > 192.168.4.127.679: . ack 2819578126 win 1024
```

```
13:59:02.405614 IP 192.168.4.20.80 > 192.168.4.127.18181: . ack 3136331014 win 4096
13:59:02.405614 IP 192.168.4.20.80 > 192.168.4.127.424: . ack 1033617559 win 3072
13:59:02.501732 IP 192.168.4.20.80 > 192.168.4.127.348: . ack 105804234 win 2048
13:59:02.502239 IP 192.168.4.20.80 > 192.168.4.127.1022: . ack 135301122 win 4096
13:59:02.505721 IP 192.168.4.20.80 > 192.168.4.127.1480: . ack 1968258928 win 1024
13:59:02.506229 IP 192.168.4.20.80 > 192.168.4.127.335: . ack 689704508 win 1024
13:59:02.506649 IP 192.168.4.20.80 > 192.168.4.127.118: . ack 1894423097 win 3072
13:59:02.506750 IP 192.168.4.20.80 > 192.168.4.127.610: . ack 976440857 win 3072
13:59:02.507176 IP 192.168.4.20.80 > 192.168.4.127.1103: . ack 2118936872 win 3072
13:59:02.510710 IP 192.168.4.20.80 > 192.168.4.127.136: . ack 1250689503 win 3072
13:59:02.511237 IP 192.168.4.20.80 > 192.168.4.127.1356: . ack 768540085 win 1024
13:59:02.511664 IP 192.168.4.20.80 > 192.168.4.127.253: . ack 1886555537 win 3072
13:59:02.603707 IP 192.168.4.20.80 > 192.168.4.127.1022: . ack 1755044930 win 4096
13:59:02.604192 IP 192.168.4.20.80 > 192.168.4.127.348: . ack 1067201206 win 4096
13:59:02.607670 IP 192.168.4.20.80 > 192.168.4.127.1103: . ack 2978564238 win 4096
13:59:02.608176 IP 192.168.4.20.80 > 192.168.4.127.610: . ack 1012051075 win 2048
13:59:02.608281 IP 192.168.4.20.80 > 192.168.4.127.118: . ack 3843913903 win 3072
13:59:02.608698 IP 192.168.4.20.80 > 192.168.4.127.335: . ack 49617302 win 3072
13:59:02.609131 IP 192.168.4.20.80 > 192.168.4.127.1480: . ack 2767970690 win 1024
13:59:02.612617 IP 192.168.4.20.80 > 192.168.4.127.253: . ack 3443207716 win 4096
13:59:02.613133 IP 192.168.4.20.80 > 192.168.4.127.1356: . ack 724519002 win 3072
13:59:02.613240 IP 192.168.4.20.80 > 192.168.4.127.136: . ack 3541921001 win 1024
13:59:02.697941 IP 192.168.4.20 > 192.168.4.127: ICMP 192.168.4.20 udp port 137 unreachable, length 36
13:59:02.704712 IP 192.168.4.20.80 > 192.168.4.127.3985: . ack 1588058631 win 3072
13:59:02.705199 IP 192.168.4.20.80 > 192.168.4.127.816: . ack 1574646301 win 4096
13:59:02.708699 IP 192.168.4.20.80 > 192.168.4.127.715: . ack 1639398926 win 1024
13:59:02.709206 IP 192.168.4.20.80 > 192.168.4.127.1067: . ack 1162558272 win 2048
13:59:02.709642 IP 192.168.4.20.80 > 192.168.4.127.514: . ack 1310657098 win 3072
13:59:02.712718 IP 192.168.4.20.80 > 192.168.4.127.7001: . ack 1474078807 win 2048
13:59:02.713224 IP 192.168.4.20.80 > 192.168.4.127.2000: . ack 1471157457 win 3072
13:59:02.713652 IP 192.168.4.20.80 > 192.168.4.127.1364: . ack 1764151888 win 2048
13:59:02.717676 IP 192.168.4.20.80 > 192.168.4.127.2201: . ack 1941551134 win 2048
13:59:02.718179 IP 192.168.4.20.80 > 192.168.4.127.222: . ack 635892973 win 4096
```

TRACE 2 : 2008-03-10-14:00.nmap_sA_dest80.pcap

```
14:00:37.877583 IP 192.168.4.127.137 > 192.168.4.20.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
14:00:37.877633 IP 192.168.4.20 > 192.168.4.127: ICMP 192.168.4.20 udp port 137 unreachable, length 36
14:00:38.335490 IP 192.168.4.127.137 > 192.168.4.20.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
14:00:38.335523 IP 192.168.4.20 > 192.168.4.127: ICMP 192.168.4.20 udp port 137 unreachable, length 36
14:00:38.792251 IP 192.168.4.127.137 > 192.168.4.20.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
14:00:38.792279 IP 192.168.4.20 > 192.168.4.127: ICMP 192.168.4.20 udp port 137 unreachable, length 36
14:00:45.310717 IP 192.168.4.20.48777 > 192.168.4.127.80: . ack 400921770 win 1024
14:00:45.311220 IP 192.168.4.127.80 > 192.168.4.20.48777: R 400921770:400921770(0) win 0
14:00:45.412238 IP 192.168.4.20.48778 > 192.168.4.127.80: . ack 1635987751 win 2048
14:00:45.412776 IP 192.168.4.127.80 > 192.168.4.20.48778: R 1635987751:1635987751(0) win 0
```