

Testing IDS rulesets with Hping

Alt.don

This is an addendum to the earlier posted Hping tutorial on packet crafting. This will hopefully show you some more uses of this rather excellent tool. Once again I have only shown some basic probes of an IDS ruleset. You can get as complex as you wish. It also serves as an excellent platform to test out your custom signatures. Anyhow how enough jabbering from me! Read on and hopefully not fall asleep.

The purpose of the following tcpdump traces, snort output, and Hping command line syntax is to demonstrate the value of Hping. It's crafted packets will allow you to test and confirm your IDS ruleset. Only the tcp protocol was used in testing for the following examples. Though one can get as creative as one wishes with the other supported protocols, and tcp fields under Hping. For the below noted snort output, Snort 2.0 build 72 was used along with the default ruleset.

For ease of viewing and understanding the below noted packets I will give a brief explanation of the fields found within the packet header itself.

Testbox sending crafted packets via Hping is 192.168.2.112 192.168.2.112 sending out a null packet

Command line syntax used for Hping and ensuing output fm Hping

```
monkeylabs:/home/don # hping 192.168.2.113 -p 22 -c 2  
HPING 192.168.2.113 (eth0 192.168.2.113): NO FLAGS are set, 40 headers + 0 data bytes
```

Tcpdump trace of outgoing packets on 192.168.2.112

```
09:15:57.034761 192.168.2.112.2796 > 192.168.2.113.22: . [tcp sum ok] win 512 (ttl 64,  
id 32865, len 40)  
0x0000 4500 0028 8061 0000 4006 743d c0a8 0270 E..(.a..@.t=...p  
0x0010 c0a8 0271 0aec 0016 1082 878f 0598 76fa ...q.....v.  
0x0020 5000 0200 080d 0000 P.....  
  
09:15:58.027608 192.168.2.112.2797 > 192.168.2.113.22: . [tcp sum ok] win 512 (ttl 64,  
id 21805, len 40)  
0x0000 4500 0028 552d 0000 4006 9f71 c0a8 0270 E..(U-...@..q...p  
0x0010 c0a8 0271 0aed 0016 2803 9aac 133d 434b ...q....(....=CK  
0x0020 5000 0200 0378 0000 P....x..
```

Explanation of packet header metrics found in the packet sent above

09:15:57.034761 This is the time that the packet was sent right down to the micro second

192.168.2.112.2796 This is the IP address of the transmitting computer, and source port

> This tells you it is being sent from the IP address on the left to the one on the right

192.168.2.113.22 This is the IP address of the destination computer and dst port

[tcp sum ok] This means that the tcp sequence number is valid

win 512 This tells the dst computer that the src computer can receive up to 512KB

ttl 64 This value represents the time in milliseconds that the packet has to reach it's destination before being discarded.

id 21805 This is the number assigned to the IP header so it can be reassembled in case of

Testing IDS rulesets with HPing Alt.don

fragmentation.

len 40 This is the overall length of the packet itself in bytes.

Will now show the packets as they are received on the destination computer and the ensuing snort alert output.

Testbox receiving crafted packets is 192.168.2.113 Tcpdump trace of incoming packets on 192.168.2.113

```
07:51:00.346081 192.168.2.112.1312 > 192.168.2.113.22: . [tcp sum ok] win 512 (ttl 64,
id 57916, len 40)
0x0000 4500 0028 e23c 0000 4006 1262 c0a8 0270 E..(<...@..b...p
0x0010 c0a8 0271 0520 0016 39d4 590a 735c 85cc ...q....9.Y.s\..
0x0020 5000 0200 9675 0000 0c8e 1600 e8a7 P.....u.....

07:51:01.342902 192.168.2.112.1313 > 192.168.2.113.22: . [tcp sum ok] win 512 (ttl 64,
id 64711, len 40)
0x0000 4500 0028 fcc7 0000 4006 f7d6 c0a8 0270 E..(....@.....p
0x0010 c0a8 0271 0521 0016 02ed 0c77 4d2e d25c ...q.!.....wM..\
0x0020 5000 0200 f38c 0000 5549 444c 0d0a P.....UIDL..
```

Snort output due to crafted packets received on 192.168.2.113

```
[**] [111:9:1] spp_stream4: STEALTH ACTIVITY (NULL scan) detection [**]
06/18-07:51:00.346081 192.168.2.112:1312 -> 192.168.2.113:22
TCP TTL:64 TOS:0x0 ID:57916 IpLen:20 DgmLen:40
***** Seq: 0x39D4590A Ack: 0x735C85CC Win: 0x200 TcpLen: 20

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED to port 22 from 192.168.2.112
(STEALTH) [**]
06/18-07:51:00.832829

[**] [111:9:1] spp_stream4: STEALTH ACTIVITY (NULL scan) detection [**]
06/18-07:51:01.342902 192.168.2.112:1313 -> 192.168.2.113:22
TCP TTL:64 TOS:0x0 ID:64711 IpLen:20 DgmLen:40
***** Seq: 0x2ED0C77 Ack: 0x4D2ED25C Win: 0x200 TcpLen: 20
```

Portscan.log entry fm 192.168.2.113

```
Jun 18 07:51:04 192.168.2.112:1316 -> 192.168.2.113:22 NULL *****
```

I will now show what happens when a XMAS packet is sent. Once again the above noted format will be used. If you become confused by the meaning of some of the packet metrics used please see the earlier explanation of the header metrics.

192.168.2.112 sending out a XMAS packet

Command line syntax used for Hping and ensuing output fm Hping Code:

```
monkeylabs:/home/don # hping -S -R -P -A -F -U 192.168.2.113 -p 22 -c 5 -t 118 -y
HPING 192.168.2.113 (eth0 192.168.2.113): RSAFFPU set, 40 headers + 0 data bytes
```

Tcpdump trace of outgoing packets on 192.168.2.112

```
08:05:08.858815 192.168.2.112.1211 > 192.168.2.113.22: SFRP [tcp sum ok]
```

Testing IDS rulesets with HPing

Alt.don

```
318976457:318976457(0) ack 1818840445 win 512 urg 0 (DF) [tos 0x10] (ttl 118, id
50387, len 40)
0x0000 4510 0028 c4d3 4000 7606 b9ba c0a8 0270 E..(..@.v.....p
0x0010 c0a8 0271 04bb 0016 1303 31c9 6c69 4d7d ...q.....1.liM}
0x0020 503f 0200 23f0 0000 0c8e 1600 e8a7 P?...#......
```

```
08:05:09.857708 192.168.2.112.1212 > 192.168.2.113.22: SFRP [tcp sum ok]
16649609:16649609(0) ack 172211276 win 512 urg 0 (DF) [tos 0x10] (ttl 118, id 30817,
len 40)
0x0000 4510 0028 7861 4000 7606 062d c0a8 0270 E..(xa@.v...-...p
0x0010 c0a8 0271 04bc 0016 00fe 0d89 0a43 bc4c ...q.....C.L
0x0020 503f 0200 4d8b 0000 5041 5353 2067 P?...M...PASS.g
```

Testbox receiving crafted packets is 192.168.2.113

Tcpdump trace of incoming packets on 192.168.2.113

```
08:05:08.858815 192.168.2.112.1211 > 192.168.2.113.22: SFRP [tcp sum ok]
318976457:318976457(0) ack 1818840445 win 512 urg 0 (DF) [tos 0x10] (ttl 118, id
50387, len 40)
0x0000 4510 0028 c4d3 4000 7606 b9ba c0a8 0270 E..(..@.v.....p
0x0010 c0a8 0271 04bb 0016 1303 31c9 6c69 4d7d ...q.....1.liM}
0x0020 503f 0200 23f0 0000 0c8e 1600 e8a7 P?...#......
```

```
08:05:09.857708 192.168.2.112.1212 > 192.168.2.113.22: SFRP [tcp sum ok]
16649609:16649609(0) ack 172211276 win 512 urg 0 (DF) [tos 0x10] (ttl 118, id 30817,
len 40)
0x0000 4510 0028 7861 4000 7606 062d c0a8 0270 E..(xa@.v...-...p
0x0010 c0a8 0271 04bc 0016 00fe 0d89 0a43 bc4c ...q.....C.L
0x0020 503f 0200 4d8b 0000 5041 5353 2067 P?...M...PASS.g
```

Snort output due to crafted packets received on 192.168.2.113

```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
06/18-08:05:08.858815 192.168.2.112:1211 -> 192.168.2.113:22
TCP TTL:118 TOS:0x10 ID:50387 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0x130331C9 Ack: 0x6C694D7D Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

```
[**] [100:1:1] spp_portscan: PORTSCAN DETECTED to port 22 from 192.168.2.112
(STEALTH) [**]
06/18-08:05:08.861384
```

```
[**] [111:6:1] spp_stream4: STEALTH ACTIVITY (Full XMAS scan) detection [**]
06/18-08:05:09.857708 192.168.2.112:1212 -> 192.168.2.113:22
TCP TTL:118 TOS:0x10 ID:30817 IpLen:20 DgmLen:40 DF
**UAPRSF Seq: 0xFE0D89 Ack: 0xA43BC4C Win: 0x200 TcpLen: 20 UrgPtr: 0x0
```

Portscan.log entry fm 192.168.2.113

```
Jun 18 08:05:12 192.168.2.112:1215 -> 192.168.2.113:22 FULLXMAS **UAPRSF
```

As seen in the above noted examples Hping is very much capable of testing out an IDS ruleset through the use of crafted packets. This is of value for the simple fact that it does confirm unequivocally that your IDS rulesets are triggering to expected stimulus such as the one's shown above. Hopefully some of you will find this somewhat useful.