Lab7

Name: 黎诗龙

SID: 11811407

2

a

A zero-day attack is an attack for a vulnerability that is unknown to the public community.

[**Refer** to P. Garcia-Teodoro, J. Diaz-Verdejo, G. MaciaFernandez, and E. Vazquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” Computers and Security, vol. 28, no. 1–2, pp. 18–28, 2009.]

Zero-day vulnerabilities can take almost any form, including SQL injection, buffer overflows, missing authorizations, etc.

[**Refer** to https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-zero-day-attack/]

b

Snort **may** catch zero-day network attacks.

The reason:

Rules are a different methodology for performing detection, which bring the advantage of 0-day detection to the table. Unlike signatures, rules are based on detecting the actual vulnerability, not an exploit or a unique piece of data. Developing a rule requires an acute understanding of how the vulnerability actually works.

[Refer to https://www.snort.org/faq/what-is-a-snort-rule]

Signature of detection is typically classified as day after detection, as actual public exploits are necessary for this type of detection to work. Anti-Virus companies utilize this type of technology for protecting their customers from virus outbreaks. As we have seen over the years this type of protection only has limited protection capabilities as the virus has already infected someone before a signatures can be written.

[Refer to https://www.snort.org/faq/what-is-a-signature]

From above we can see that we can use Snort rules to detect 0-day attack.

c

Given that:

$$\frac{TP+FN}{TP+FN+FP+TN} = 0.1\% = 0.001(1)$$

$$\textbf{true positive rate} = \frac{TP}{TP+FN} = 0.95(2)$$

$$\textbf{alarm is an attack} = \frac{TP}{TP+FP} = 0.95(3)$$

Solution:

All we need is to get $\frac{FP}{FP+TP}$.

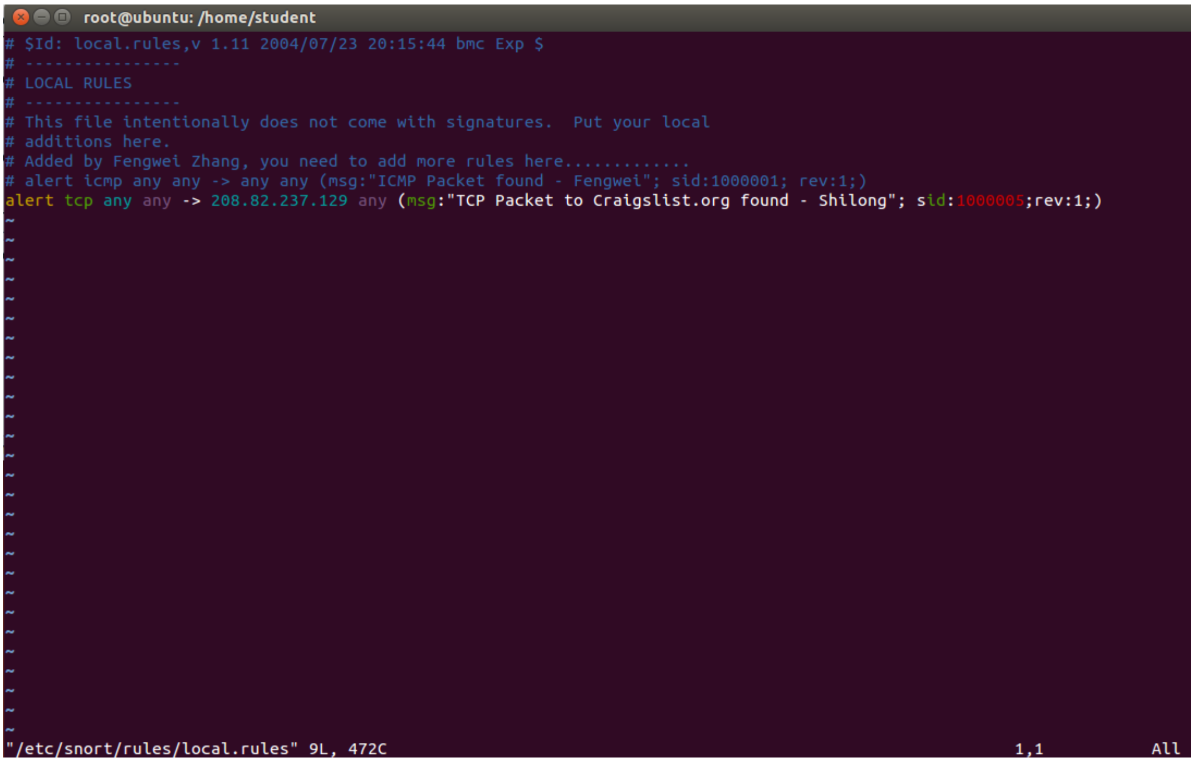
$$\frac{FP}{FP+TP} = 1 - \frac{TP}{FP+TP} = 0.05$$

The false alarm rate is `5%`.

3

a

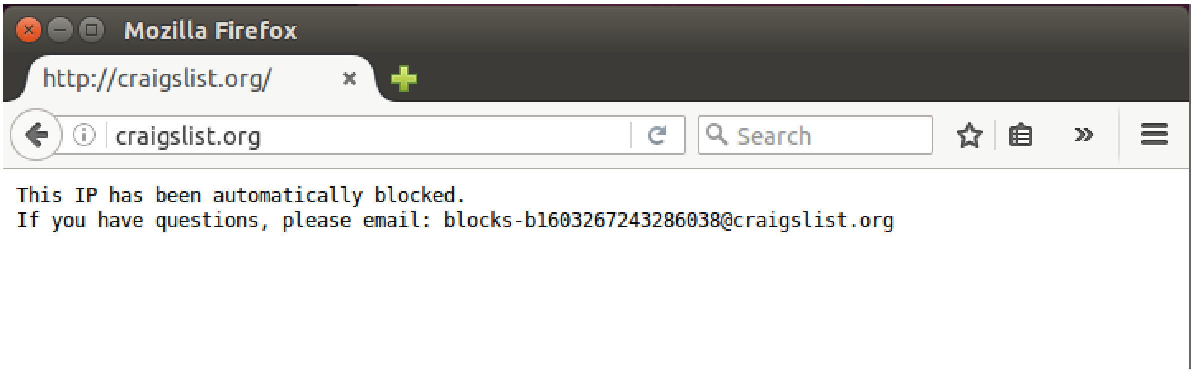
I add this rule, `alert tcp any any -> 208.82.237.129 any (msg:"TCP Packet to Craigslist.org found - Shilong"; sid:1000005;rev:1;)`, into the `local.rules`.



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
# Added by Fengwei Zhang, you need to add more rules here.............
# alert icmp any any -> any any (msg:"ICMP Packet found - Fengwei"; sid:1000001; rev:1;)
alert tcp any any -> 208.82.237.129 any (msg:"TCP Packet to Craigslist.org found - Shilong"; sid:1000005;rev:1;)
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/snort/rules/local.rules" 9L, 472C                                                   1,1           All
```

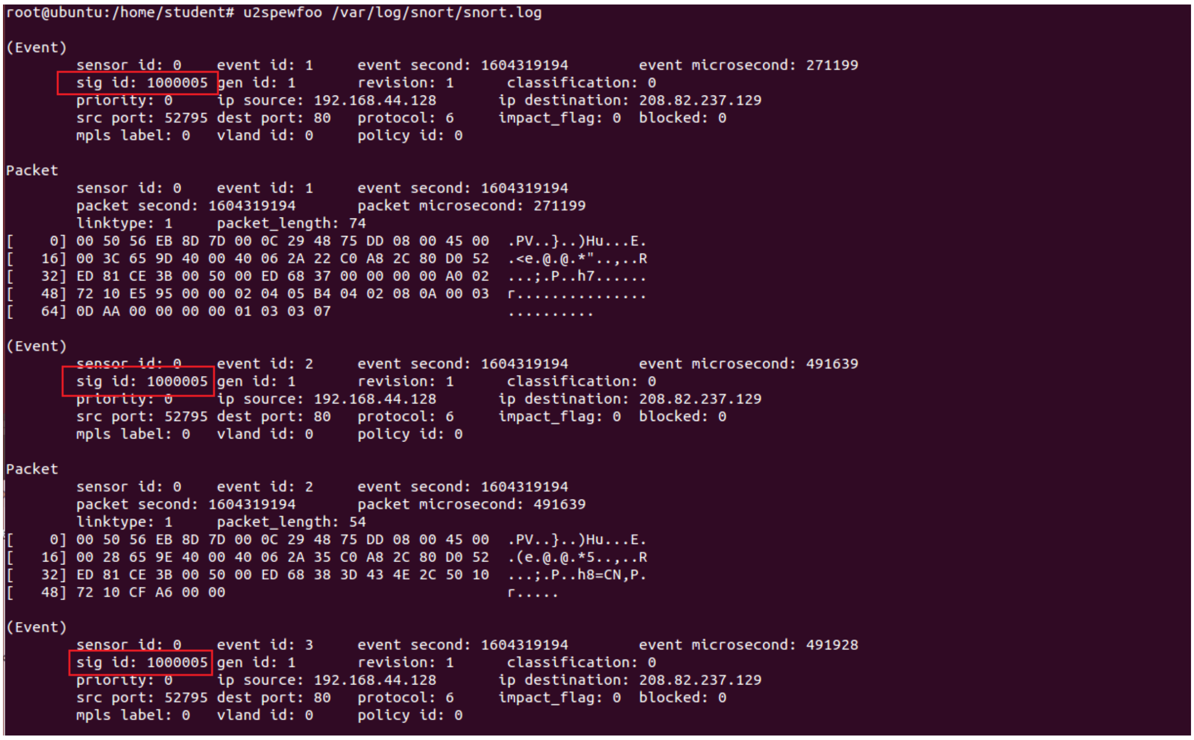
b

I open the firefox explorer to visit `craigslist.org`.



```
This IP has been automatically blocked.
If you have questions, please email: blocks-b1603267243286038@craigslist.org
```

C



```
root@ubuntu:/home/student# u2spewfoo /var/log/snort/snort.log

(Event)
        sensor id: 0    event id: 1     event second: 1604319194        event microsecond: 271199
        sig id: 1000005 gen id: 1       revision: 1      classification: 0
        priority: 0     ip source: 192.168.44.128       ip destination: 208.82.237.129
        src port: 52795 dest port: 80   protocol: 6     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0

Packet
        sensor id: 0    event id: 1     event second: 1604319194
        packet second: 1604319194       packet microsecond: 271199
        linktype: 1     packet_length: 74
[    0] 00 50 56 EB 8D 7D 00 0C 29 48 75 DD 08 00 45 00  .PV..}..)Hu...E.
[   16] 00 3C 65 9D 40 00 40 06 2A 22 C0 A8 2C 80 D0 52  .<e.@.@.*"..,..R
[   32] ED 81 CE 3B 00 50 00 ED 68 37 00 00 00 00 A0 02  ...;.P..h7......
[   48] 72 10 E5 95 00 00 02 04 05 B4 04 02 08 0A 00 03  r...............
[   64] 0D AA 00 00 00 00 01 03 03 07                    ..........

(Event)
        sensor id: 0    event id: 2     event second: 1604319194        event microsecond: 491639
        sig id: 1000005 gen id: 1       revision: 1      classification: 0
        priority: 0     ip source: 192.168.44.128       ip destination: 208.82.237.129
        src port: 52795 dest port: 80   protocol: 6     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0

Packet
        sensor id: 0    event id: 2     event second: 1604319194
        packet second: 1604319194       packet microsecond: 491639
        linktype: 1     packet_length: 54
[    0] 00 50 56 EB 8D 7D 00 0C 29 48 75 DD 08 00 45 00  .PV..}..)Hu...E.
[   16] 00 28 65 9E 40 00 40 06 2A 35 C0 A8 2C 80 D0 52  .(e.@.@.*5..,..R
[   32] ED 81 CE 3B 00 50 00 ED 68 38 3D 43 4E 2C 50 10  ...;.P..h8=CN,P.
[   48] 72 10 CF A6 00 00                                r.....

(Event)
        sensor id: 0    event id: 3     event second: 1604319194        event microsecond: 491928
        sig id: 1000005 gen id: 1       revision: 1      classification: 0
        priority: 0     ip source: 192.168.44.128       ip destination: 208.82.237.129
        src port: 52795 dest port: 80   protocol: 6     impact_flag: 0  blocked: 0
        mpls label: 0   vland id: 0     policy id: 0
```