CS315 · Computer Security

Lab 7

胡玉斌 / 11712121

November 20, 2020

1 Read the lab instructions above and finish all the tasks.

Done

2 Answer the questions and justify your answers.Simple yes or no answer will not get any credits.

2.1 What is a zero-day attack?

- A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who should be interested in mitigating the vulnerability (including the vendor of the target software).
- Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.
- The term "zero-day" originally referred to the number of days since a new piece of software was released to the public, so "zero-day" software was software that had been obtained by hacking into a developer's computer before release. Eventually the term was applied to the vulnerabilities that allowed this hacking, and to the number of days that the vendor has had to fix them. Once the vendor learns of the vulnerability, the vendor will usually create patches or advise workarounds to mitigate it.

2.2 Can Snort catch zero-day network attacks? If not, why not? If yes, how?

- No
- Snort is one of the most popular open-source and rule-based IDSs.
- Its rules recognise malicious network packets by matching the current packet against predefined rules and cannot detect zero-day attacks but produce a high FPR due to its methodology for identifying attack signatures.

2.3 Given a network that has 1 million connections daily where 0.1% (not 10%) are attacks. If the IDS has a true positive rate of 95%, and the probability that an alarm is an attack is 95%. What is false alarm rate? (You may use the math approach from the slides.)

$$\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} = 95\%$$

when TP = 950, FP = $999000 * r$, so we have:

$$\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} = 95\%$$

So false alarm rate is = 0.005005%.

3 Write a rule that will fire when you browse to craigslist.org or another particular website from the machine Snort is running on; it should look for any outbound TCP request to craigslist.org and alert on it.

3.1 The rule you added(from the rules file)

- We browse to sustech.edu.cn

```
alert tcp any any -> any any (msg:"SUSTech Packet found - Eveneko"; content:"
    sustech.edu.cn"; sid:1000002; rev:1;)
```

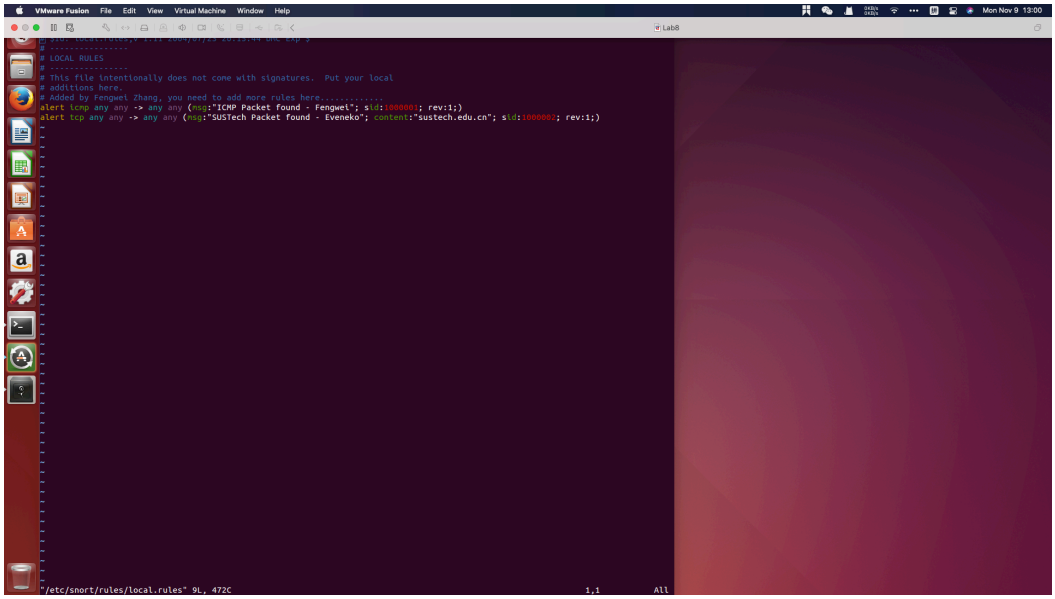

Figure 1: rule

3.2 A description of how you triggered the alert

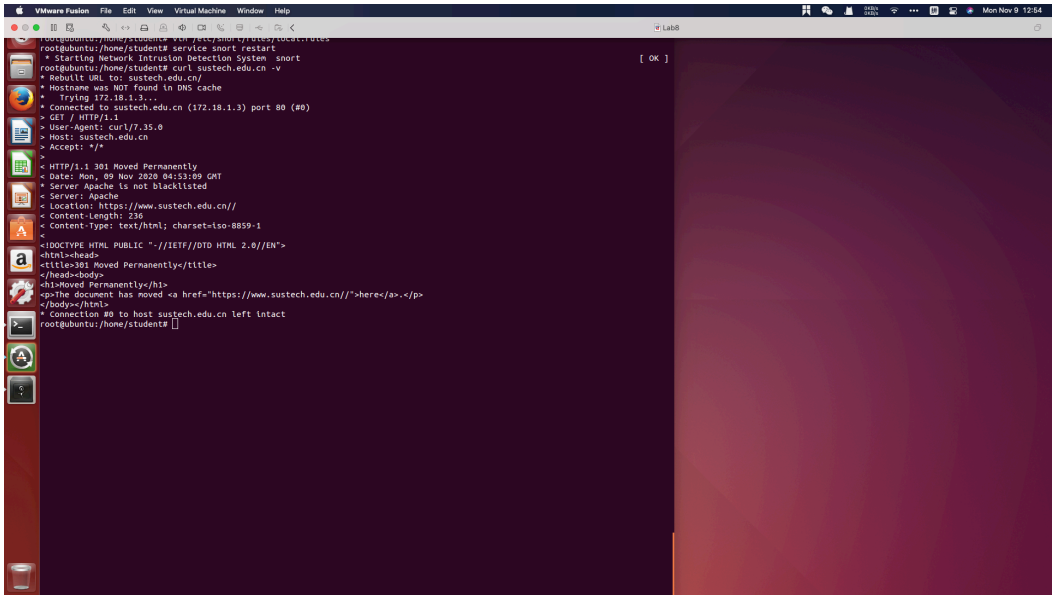

Figure 2: trigger

3.3 The alert itself from the log file (after converting it to readable text)

```
(Event)
        sensor id: 0    event id: 2     event second: 1604897588        event microsecond: 935330
        sig id: 1000002 gen id: 1       revision: 1      classification: 0
        priority: 0     ip source: 172.18.1.3   ip destination: 192.168.249.4
        src port: 80    dest port: 45093        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: 1604897588
        packet second: 1604897588       packet microsecond: 935330
        linktype: 1     packet_length: 495
[    0] 00 0C 29 DC 41 79 FA FF C2 A1 26 64 08 00 45 00  ..).Ay....&d..E.
[   16] 01 E1 3C 4F 00 00 3D 06 D9 05 AC 12 01 03 C0 A8  ..<O..=.........
[   32] F9 04 00 50 B0 25 53 CC C0 2A 49 D7 18 24 80 18  ...P.%S..*I..$..
[   48] 00 E3 CE 0A 00 00 01 01 08 0A 7D C6 FC 65 00 20  ..........}..e.
[   64] F9 CF 48 54 54 50 2F 31 2E 31 20 33 30 31 20 4D  ..HTTP/1.1 301 M
[   80] 6F 76 65 64 20 50 65 72 6D 61 6E 65 6E 74 6C 79  oved Permanently
[   96] 0D 0A 44 61 74 65 3A 20 4D 6F 6E 2C 20 30 39 20  ..Date: Mon, 09
[  112] 4E 6F 76 20 32 30 32 30 20 30 34 3A 35 33 3A 30  Nov 2020 04:53:0
[  128] 39 20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41  9 GMT..Server: A
[  144] 70 61 63 68 65 0D 0A 4C 6F 63 61 74 69 6F 6E 3A  pache..Location:
[  160] 20 68 74 74 70 73 3A 2F 2F 77 77 77 2E 73 75 73   https://www.sus
[  176] 74 65 63 68 2E 65 64 75 2E 63 6E 2F 2F 0D 0A 43  tech.edu.cn//..C
[  192] 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 32  ontent-Length: 2
[  208] 33 36 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65  36..Content-Type
[  224] 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61  : text/html; cha
[  240] 72 73 65 74 3D 69 73 6F 2D 38 38 35 39 2D 31 0D  rset=iso-8859-1.
[  256] 0A 0D 0A 3C 21 44 4F 43 54 59 50 45 20 48 54 4D  ...<!DOCTYPE HTM
[  272] 4C 20 50 55 42 4C 49 43 20 22 2D 2F 2F 49 45 54  L PUBLIC "-//IET
[  288] 46 2F 2F 44 54 44 20 48 54 4D 4C 20 32 2E 30 2F  F//DTD HTML 2.0/
[  304] 2F 45 4E 22 3E 0A 3C 68 74 6D 6C 3E 3C 68 65 61  /EN">.<html><hea
[  320] 64 3E 0A 3C 74 69 74 6C 65 3E 33 30 31 20 4D 6F  d>.<title>301 Mo
[  336] 76 65 64 20 50 65 72 6D 61 6E 65 6E 74 6C 79 3C  ved Permanently<
[  352] 2F 74 69 74 6C 65 3E 0A 3C 2F 68 65 61 64 3E 3C  /title>.</head><
[  368] 62 6F 64 79 3E 0A 3C 68 31 3E 4D 6F 76 65 64 20  body>.<h1>Moved
[  384] 50 65 72 6D 61 6E 65 6E 74 6C 79 3C 2F 68 31 3E  Permanently</h1>
[  400] 0A 3C 70 3E 54 68 65 20 64 6F 63 75 6D 65 6E 74  .<p>The document
[  416] 20 68 61 73 20 6D 6F 76 65 64 20 3C 61 20 68 72   has moved <a hr
[  432] 65 66 3D 22 68 74 74 70 73 3A 2F 2F 77 77 77 2E  ef="https://www.
[  448] 73 75 73 74 65 63 68 2E 65 64 75 2E 63 6E 2F 2F  sustech.edu.cn//
[  464] 22 3E 68 65 72 65 3C 2F 61 3E 2E 3C 2F 70 3E 0A  ">here</a>.</p>.
[  480] 3C 2F 62 6F 64 79 3E 3C 2F 68 74 6D 6C 3E 0A     </body></html>.
```

Figure 3: log