A09 – IDS Rules 2

**10 points**  
Turn in a Word or PDF document to the D2L Dropbox

# Overview

In this lab you'll be writing more IDS rules for Suricata.

For parts 5-7, you will be using the Suricata VM in the IA Lab. The username is *root* and the password is *Password1!*

The pcaps are provided on the VM in the IA Lab. You can also download the pcaps locally at <https://files.dakotastate.net/ids_pcaps.zip>

**Complete *Try It 4* from the slides.** Fill in the components listed on the slide including the content and options related to that content.

1. (1 point) Example\_4.pcap, packet 10

dsize:12; content: “nocookie”;

1. (1 point) Example\_3.pcap, packet 185

dsize:102; content: “SMB”; content: “| 6c 00 00 90 73 00 61 00 72 00 70 00 63 00 00 00 |”; distance:0;

1. (1 point) Example\_5.pcap, packet 14

dsize: 260; content: ”AMD phenom | 28 |”; nocase; content: ”tm| 28 |”; distance:0; nocase; content: ”9550 Quad| 2d |Core Processor”; distance:0; nocase;

**Complete *Try It 5* from the slides**. Fill in the given content section

1. (1 point) Example\_6.pcap, packet 41

Content:”| 00 01 00 00 00 01 |”; offset:45; depth:51; content:”| 02 | eu | 00 | “; distance:0; within:23;

**Complete *Try It 6* from the slides.** Provide the entire rule. Be sure to include the metadata in the rule headers as well as content. **Test your rules in the Suricata VM and provide a screenshot for each.**

1. (2 points) Example\_10.pcap, packet 16011 - Write a rule that detects if someone is attempting to log in to an FTP server as admin.

Alert ftp $Home\_Net any -> $Home\_Net 21 (msg: “FTP login attempt: User-Admin”; flow: from\_client, established; content:”USER admin”; nocase; classtype: admin-login; sid:1000003; rev: 1; metadata: created\_at 2020\_4\_7;)

1. (2 points) Example\_11.pcap, - Write a rule that detects a suspicious user agent found in example\_11.pcap

Alert http $Home\_Net any -> $External\_net 80 (msg: “Suspicious User-Agent (BlackSun) web access”; flow: to\_server, established; content:”User| 2d |Agent| 3a | BlackSun”; nocase; classtype: bad-unknown; sid:1000004; rev: 1; metadata: created\_at 2020\_4\_7😉

1. (2 points) Example\_12.pcap, packet 10 - Write a rule that detects the nitol command and control traffic.

Alert tcp $Home\_Net any -> $External\_Net 6666 (msg: ”Nitol Command and Control detected”; flow: to\_server, established; dsize: 520; content: “RON| 2d |AC13BF686B1”; classtype: bad-unknown; sid: 1000005; rev:1; metadata: created\_at 2020\_4\_7😉

-------------------------------------------

To test your rules in the Suricata VM, complete the following steps:

1. Enter your rules in the custom.rules file, one on each line. Be sure they have unique SIDs.
   1. The command line text editors *Nano* and *VI* are both installed on the VM.
2. Run the runtest.sh script, supplying the path to the pcap you would like to test the rules against.
   1. For example: ./runtest.sh pcaps/example\_1.pcap