I’m currently locked out of my webmail, and the ialab. I just reset my password tonight and the only university resource I can access since then is the page at myds.edu where you reset your password. So, I’ve reset it multiple times, but I can’t log in anywhere else. I’m going to call in to IT in the morning to see what is going on. I may not be able to log back into d2l until this gets sorted, so rip.   
  
A08 – IDS Rules 1

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

# Overview

In this lab you'll be writing IDS rules for Suricata based on the components that were covered in class so far. There are more components to IDS rule writing than was discussed that will help make the rules more specific, but we are going to take things slow and ease into the many components that go into an IDS rule.

For part 9, 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 1 from the slides.** Provide the first portion of an IDS rule with proper syntax that contains the action, protocol, direction, and source and destination IPs and ports.

1. (1 point) Example\_1.pcap, packet 26

alert http $Home\_Net any -> 104.27.161.97 80

1. (1 point) Example\_2.pcap, packet 2

alert icmp 61.144.195.93 any -> !61.144.195.93 any

1. (1 point) Example\_3.pcap, packet 10

alert smb [$External\_net, $Home \_Net] any -> $Home\_Net 445

**Complete *Try It 2* from the slides**. Provide the message and flow for the following cases.

1. (1 point) You are writing a signature for a WannaCry DNS Lookup

msg:”TRJN:WANNACRY-DNS-LOOKUP”;

flow:to\_server,established;

1. (1 point) You are writing a signature for an executable payload from the Neutrino Exploit Kit as it enters the network

msg:"EXPLOIT-KIT Neutrino exploit kit landing page";   
flow:to\_client,established;

**Complete *Try It 3* from the slides.** Provide the entire rule. Be sure to include the metadata in the rule headers as well as content.

1. (1 point) Example\_1.pcap, packet 26 - Write a signature that detects request for Midco-ad-website.jpg

allow http $Home\_Net any -> $External\_Net 80 (msg:”HTTP GET FILE:midco-ad-website.jpg”; flow:from\_client,established; content:”Midco-ad-website.jpg”; nocase; fast\_pattern:only; classtype:not-suspicious; sid:1000000; rev:1; metadata:created\_at 2020\_03\_31, updated\_at\_2020\_03\_31;)

1. (1 point) Example\_3.pcap, packet 10 - Write a signature that detects SMB Negotiation requests for LANMAN1.0

alert smb [$External\_net, $Home \_Net] any -> $Home\_Net 445 (msg:”TRJN:WANNACRY-DNS-LOOKUP”; flow: to\_server, established; content:”LANMAN1.0”; nocase; fast\_pattern: only; classtype: trojan-activity; sid:1000001; rev:1; metadata: created\_at 2020\_03\_31, updated\_at\_2020\_03\_31;)

1. (1 point) Example\_4.pcap, packet 10 - Write a signature that detects this packet. Be sure to use content that seems to be unique to it.

I don’t understand why this packet is of interest. I’ve been googling around for the last couple days trying to figure out (1) if nocookie has any greater meaning, (2) why is there a tcp connection over port 80 that isn’t http, (3) does the port 1030 have any known exploits/vulnerabilities, services, etc. I have found nothing noteworthy – so I’m not sure what to put in the msg.  
allow tcp $Home\_Net any -> $External\_Net 80 (msg:”TCP connection:clien\_ port\_1030 to server\_port\_80, content:nocookie”; flow: to\_server, established; content:”nocookie”; nocase; fast\_pattern:only; classtype:not-suspicious; sid:1000002; rev:1; metadata:created\_at 2020\_03\_31, updated\_at\_2020\_03\_31;)

**Test your rules**

1. (2 points) Using the Suricata VM and the pcaps, test your rules from questions 6, 7, and 8. Provide screenshots of the output/alerts from all three rules.

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

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

# alert tcp $HOME\_NET 23 -> $EXTERNAL\_NET any

# (msg:"GPL TELNET Bad Login";

# flow:from\_server,established; content:"Login

# incorrect"; nocase; fast\_pattern:only;

# classtype:bad-unknown; sid:2101251; rev:9;

# metadata:created\_at 2010\_09\_23, updated\_at

# 2010\_09\_23;)