



Assignment 5 - IDS Signatures

[Submit Assignment](#)

Due Oct 20 by 11:59pm **Points** 7 **Submitting** a file upload
Available after Oct 12 at 12am

In each of these scenarios, come up with a Snort signature that would match the traffic. Assume that HOME_NET, EXTERNAL_NET, and HTTP_PORTS are correctly defined. Assume no other variables are defined.

- 1) [1 point] You have been alerted that 10.10.27.1 is a malicious actor targeting web services. Write a signature that alerts on accesses from this host to any local web service.
- 2) [2 points] Your organization recently noticed that malicious actors were scanning for phpMyAdmin at "/phpMyAdmin/scripts/setup.php" on our web servers. The scan engine did not set a User-Agent. Write an alert for whenever an external host tries to fetch that URI without a User-Agent set. Test with [http.pcap](#) 
- 3) [2 points] Last May a phishing attack was launched where the attacker got multiple users to add a malicious service as a trusted service on their Google account. The attack required the victim to click on a link to "https://accounts.google.com/o/oauth2/auth". Write a signature that finds all email with a link to that address. Test with [smtp.pcap](#) 
- 4) [2 points] You are looking for data inside the friends lists on Yahoo! Messenger packets. The protocol is documented here: <http://libyahoo2.sourceforge.net/ymsg-9.txt> (<http://libyahoo2.sourceforge.net/ymsg-9.txt>). Write a rule that will identify Yahoo messenger packets with a service of YAHOO_SERVICE_LIST. You can test this against [ymsg2.pcap](#) 