Ground Rules. You may choose to work with one other student if you wish. Only one submission is required per group, please ensure that both group members names are on the submitted copy. Work must be submitted in hard copy by the start of class.

1) Firewall Schmirewall. Sarah is installing a stateful network firewall for her company. Being familiar with the principle of fail-safe defaults, she has configured the firewall to DENY all packets. Now she needs to identify the minimal access rules that will allow her organization to use its Internet connection. For example, her organization will need to be able to send and receive email through the firewall, and uses a central mail server at IP address 10.1.100.100. So she has added rules to the firewall that look like this:

<table>
<thead>
<tr>
<th>SRC ADDR</th>
<th>DEST ADDR</th>
<th>SRC PORT</th>
<th>DST PORT</th>
<th>PROTOCOL</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.100.100</td>
<td>*</td>
<td>*</td>
<td>sendmail</td>
<td>TCP</td>
<td>ALLOW</td>
</tr>
<tr>
<td>*</td>
<td>10.1.100.100</td>
<td>*</td>
<td>sendmail</td>
<td>TCP</td>
<td>ALLOW</td>
</tr>
</tbody>
</table>

The organization has determined that it will also require the following kinds of internet access:

- Incoming SSH access to a VPN server, at 10.1.100.200.
- Access to the web, through a proxy that whitelists approved sites, at 10.1.200.200.
- Outgoing SSH access to three client sites: 0.1.2.3, 42.42.42.42, and 3.14.15.9.

List the minimal set of firewall rules necessary to allow these connections (5 pts). List some potential vulnerabilities associated with this ruleset (3 pts). Can the firewall and proxy servers defend against these vulnerabilities (2 pts)?

2) False Positive Answer. Anderson’s chapter 10 details several ways to defeat physical intrusion detection systems (a.k.a. “burglar alarms”). One of the common ones is to artificially create “false” alarms so that the true alarm is ignored. Let’s investigate this idea with respect to logical intrusion detection systems.

(a - 2 pts) An old Snort rule says that any HTTP packet that includes “/..%c0%af../” should trigger an alarm, as an attempted IIS exploit. Explain why in “normal” usage this rule would have a low false positive rate.

(b - 5 pts) Suppose Eve discovers a web server, vulnerable.org that is vulnerable to the IIS unicode exploit and she wants to exploit the hole without having it noticed. What are a few ways Eve can temporarily increase the false positive rate at vulnerable.org for the rule, without getting her IP address noticed?

(c - 3 pts) What can you conclude about “advertised” false positive and false negative rates?
3) Virus Virii Sam has invented a brand-new virus detector, ViruSniff, and he claims it is 100% effective - if executable $F$ is a virus, then ViruSniff($F$) will output “VIRUS!!!”.

(a - 2 pts) Does ViruSniff violate the undecidability of the halting problem? Why or why not? (Hint: is there a simple program that can do exactly what Sam says ViruSniff can do?)

(b - 4 pts) Some hackers reverse engineer ViruSniff and post its algorithm online: it turns out that ViruSniff does processor emulation of the first 10000 instructions of an executable, and then applies a fancy signature matching algorithm (that no one seems to understand) to the sequence of instructions and memory changes to decide if the program is a virus or not. Explain how to change any program that runs for at least 10001 instructions, and does not trigger the VIRUS!!! alert, to propagate a virus such that the altered program will also fail to trigger the alert. What does your strategy say about Sam’s claim?

(c - 4 pts) Since you’ve shown that ViruSniff has some false negatives, how would you go about changing ViruSniff to detect a virus that uses your strategy? What effect would this change have on false positives?

Paper Review If you are a graduate student, you are expected to also include with this exercise set a paper review of one of the papers posted as graduate reading over these two weeks. Your paper review is not supposed to be a full paper in and of itself, but rather a summary in your own words and some evidence that you’ve thought about what the paper is trying to do, if they achieve their goals, how useful their goals are, and how it could be improved. Your paper review should have the following components.

- A brief summary in your own words about what the paper was about. You should cover what problem the paper was trying to solve or highlight, how the authors proposed achieving their goals, and how the authors evaluated their success. This should NOT simply be a re-statement of the abstract hit with a thesaurus until un-recognizable, I do not mind if you did not fully understand the paper, if something was confusing, or you did not understand a concept, feel free to state that. (1-2 paragraphs)

- State one problem with the paper. Every paper has a problem, be it an evaluation that does not actually measure what it should, a poor assumption, an incorrect threat model, an obvious attack/defense, etc. Find one thing that you think is a flaw in the paper, and briefly explain why you think it is a flaw. (2-3 sentences)

- State two possible things that could be done for future work. This could be expanding the attack/defense to work under different assumptions or in different deployments. It could be a different set of evaluations. It could be an improvement to how the system is constructed. Try to be specific. (1-2 sentences each)

Choose a paper from the weeks listed as “Malware and Botnets” or “Firewalls and IDS”.