Network Security
Homework Assignment 5

Due date: December 9th
5 points

CS4285 and CS5285
2016 Fall

In your submission, please provide for each problem a very brief explanation of your solution.

Please feel free to provide feedback regarding the course at:
https://goo.gl/forms/olaV2l3daIVX6tcI2

Problem 1 – DMZ (0.5 point)

In this assignment, you have to build a Demilitarized Zone (DMZ) for a company. Which of the following computers should be in the DMZ and which should be in the internal network:

- printer server for local computers (LPR on TCP port 515)
- webserver for the company's public website (HTTP on TCP port 80)
- fileserver storing sensitive information (SMB on TCP port 445)
- mail server (SMTP on TCP port 25)?

Problem 2 – DMZ Firewall (2 points)

Suppose that separation is implemented using a single firewall (i.e., "three-legged" model), and the addresses of the DMZ and the internal network are 203.0.113.0/25 and 203.0.113.128/25, respectively. Assign arbitrary IP addresses to the servers that you have placed in either the DMZ or the internal network in Problem 1.

Formalize firewall rules that implement the following informal requirements for TCP traffic:

- Do not allow connections from the Internet or the DMZ to the internal network.
- Allow connections from the Internet to the servers in the DMZ (but only to the ports that are used by the services provided by these servers, see Problem 1), but not to any other host or port.
- Allow connections from the internal network to the DMZ and the Internet.
- Allow connections from the DMZ to the Internet.

Describe your rules using a list of `iptables` commands, each of which takes the following form:

`iptables -A FORWARD -p tcp --dport` ***PORT*** `--source` ***IP*** `--destination` ***IP*** `-m state --state` ***STATES*** `-j` ***ACTION***

where

- ***PORT*** is a destination port number (0 … 65535)
- ***IP*** is a range of IP addresses given using variable-length subnet mask (e.g., 203.0.113.0/25)
- ***STATES*** is either
  - `NEW` (first packet within a TCP connection)
  - `ESTABLISHED` (subsequent packets within a TCP connection)
  - `NEW,ESTABLISHED` (packet is either `NEW` or `ESTABLISHED`).
- ***ACTION*** is either `ACCEPT` or `DROP`.

If a packet matches multiple rules in the list, then the action of the first matching rule is applied. If a packet matches none of the rules, then the default policy is applied, which can be set using:
`iptables -P FORWARD` ***ACTION***

Problem 3 – Intrusion Detection (1.5 point)

For additional security, traffic going through the firewall is monitored using the Snort network intrusion-detection system.

- Write a Snort rule that raises an alarm when someone not from the internal network tries to access the page `admin.php` on the webserver using HTTP.
- Write a Snort rule that raises an alarm when a computer from the internal network tries to connect to an SMTP server other than the dedicated mail server.

Note that ranges of IP addresses can be specified in Snort using variable-length subnet masks (e.g., 203.0.113.0/25).

Problem 4 – Taint Analysis (1 point)

Which of the variables defined in the following piece of Java code can be considered tainted (e.g., for the purpose of specifying which file to include in Java Server Pages)?

```
String variable0 = "default";
Scanner scanner = new Scanner(System.in);
String variable1 = scanner.next();
String variable2 = variable1 + variable0;
String variable3 = (variable1 == "test") ? "this" : "that";
String variable4 = variable2.substring(variable1.indexOf("/"));
String variable5 = variable2.toUpperCase();
String variable6 = variable3 + variable5;
String variable7 = variable3 + variable0;
String variable8 = null;
switch (variable5) {
  case "a":
    variable8 = variable3;
    break;
  default:
    variable8 = variable7;
}
```