Understanding IPTables

Due: September 25th

A host-based firewall is an important part of a defense-in-depth strategy, and IPtables is the firewall baked in to the Linux kernel. Below is a minimalist firewall script, but what exactly is it doing? For the first part of this assignment, you should write a short explanation of what that command is doing. Add these explanations in as comments to the script. Use the documentation provided in the Canvas module to help determine what each line of the script does. The first few lines of the script have been done for you as an example.

After you've completed the first part of the assignment, answer the questions on the second page of this homework document.

Submit your answers on Canvas; please include the questions to make grading easier on the TA!

Firewall Script

```
#!/bin/bash
# tells the program loader to use BASH (Bourne Again Shell) for running the script

IPTABLES="/sbin/iptables"
# assigns the value /sbin/iptables to the variable IPTABLES

$IPTABLES –F
# flushes all firewall rules

$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD

$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD DROP

$IPTABLES -A INPUT -i lo -j ACCEPT

$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

$IPTABLES -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

$IPTABLES -A INPUT -p tcp -j LOG

$IPTABLES -A INPUT -j REJECT --reject-with icmp-host-prohibited
```

After you've gone through and made a short description of what each line of the firewall script is doing, answer the questions below.

1. What kind of firewall does IPTables implement?

2. In order to run this script, we would need to make it executable; assuming the script is name "firewall.sh", how would we go about making this script executable?

3. What line would you add to this script to create rules for:
    a. DNS?
    b. HTTP?
    c. HTTPS?
    d. SMTP?