Design Document

Intrusion Prevention System

BCIT

February 22, 2016
Authored by: Marc Vouve

Design Document

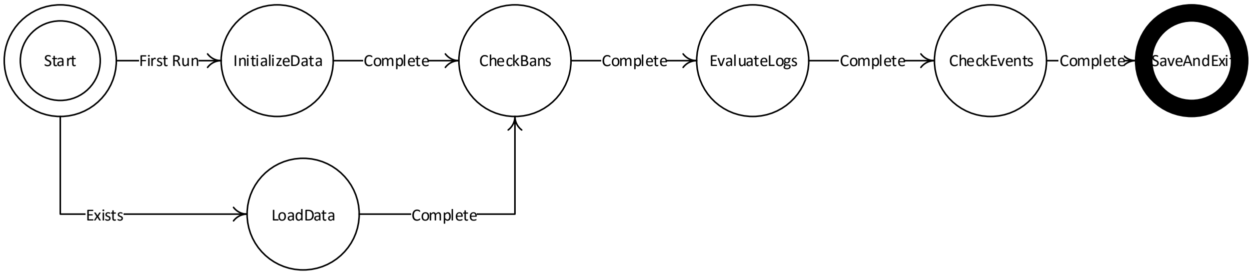
Intrusion Prevention System

Primary Application

The IPS will be triggered periodically by *cron*. For this implementation, there will be an emphasis on processor time over secondary memory space used and certain aspects of the IPS's state will be saved between uses. When a violation occurs, the IPS will cause *IPTables* to issues a ban via *NetFilter*.

Upon closing the program will create a manifest file that stores information about logs read so far, allowing the program to continue execution from the same point if re-run. This manifest file will contain information on the position reached in the log file, resent connection attempts, and current bans issued by the IPS.

Finite State Machine



State	Description	Event
Start	Program initializes, check if there is a data-file for the program	**First Run:** There is no data file. **Exists:** There is a data file.
InitializeData	Build data structures that would otherwise be loaded from the program info file	**Complete:** Data has been initialized to the correct values.
CheckBans	Check bans analyses the current bans to see if any should expire.	**Complete:** Finish checking bans
Evaluate Logs	Check the log file to see if there are new entries, and collects them.	**Complete:** EOF has been reached.
Check Events	Checks events found by check events, and prior invocations of this program. If a client has more failed attempts than allowed ban them.	**Complete:** All events checked.
SaveAndExit	Save information about execution to a file	
Load Data	Load data from file.	**Complete:** Program info loaded

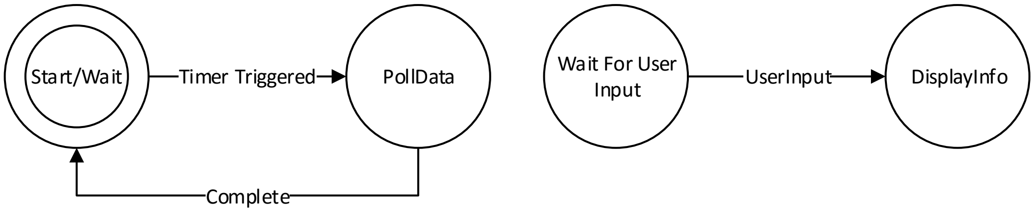
Pseudocode

1. Program is initialized by cron
2. If program manifest file exists, load the manifest file to establish current running parameters of the program. This will include the number of lines read last time the file was loaded and current list of eternal login attempts
3. Otherwise initialize program with default values.
4. Check list of banned IP addresses, if any are ready to be unbanned, unban them.
5. Evaluate logs for new entries, if any clients have committed a rule violation, ban them using IPTables. Log that this client has been banned.
6. Save current state of program to manifest file and exit

Web GUI

The web GUI displays information saved between executions of the cron job. There web GUI occupies 2 separate states at once independently as it receives and deals with information from the user and the IPS separately.

Finite State Machine



State	Description	Event
Start/Wait	Idle state for waiting for server info	**Timer Triggered:** Triggered by a timer to recheck the server for updates.
PollData	Polls the IPS for an updated manifest and saves it.	**Complete:** Webpage received updated page.
Wait for User Input	Waits for the to click one of the hosts listed on the web page	**UserInput:** User has selected a host.
DisplayInfo	Display info about about the selected state	

Pseudo Code

1. Load data from IPS and list hosts that have received requests as buttons.
2. Set timer to keep polling server for updated list
3. If a ip is selected list events associated with that IP in a table.