Final NSM Project

Andrew Maddox

University of Advancing Technology

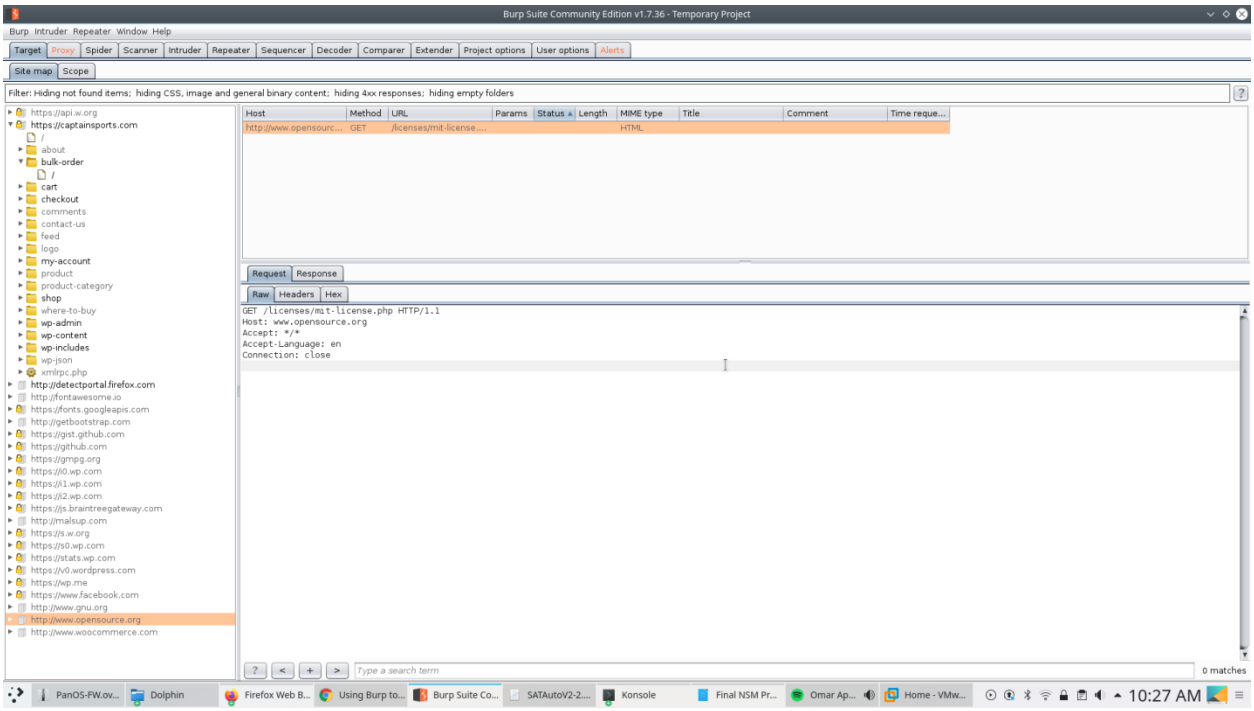
Author Note

This paper was prepared for NTS350, taught by Michael Vasquez, Title Final NSM Project.

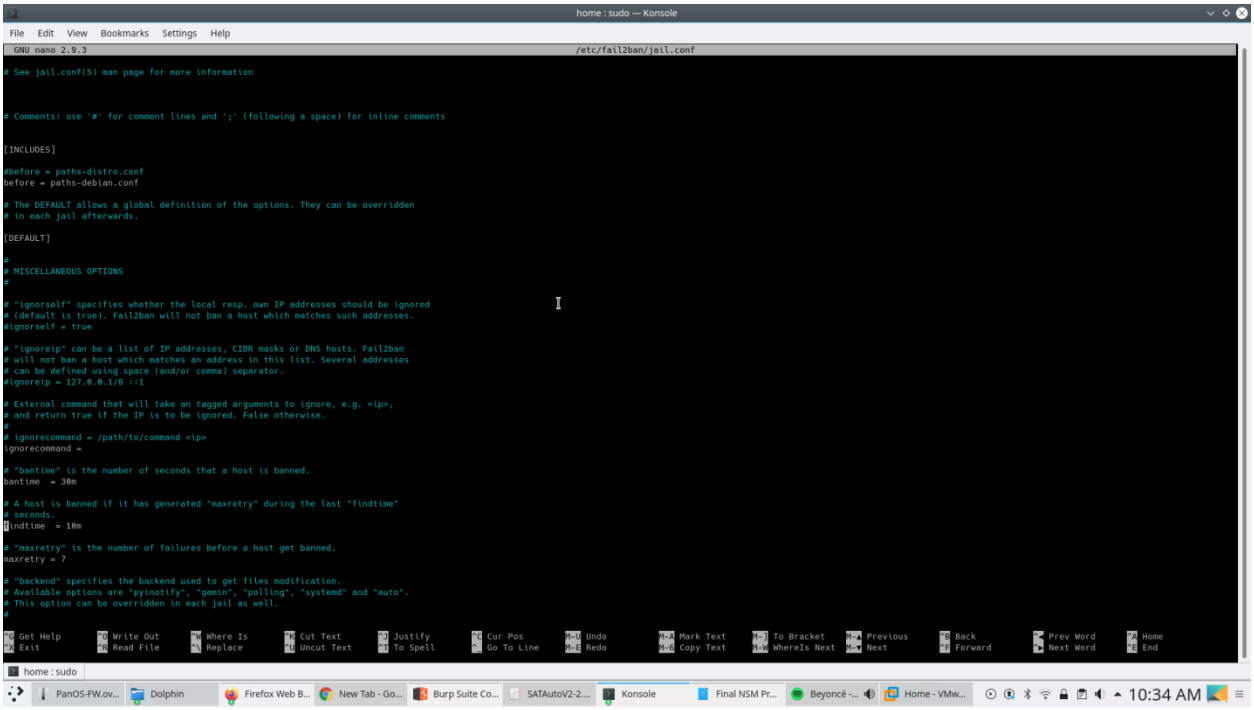
Network Security Monitoring Tools

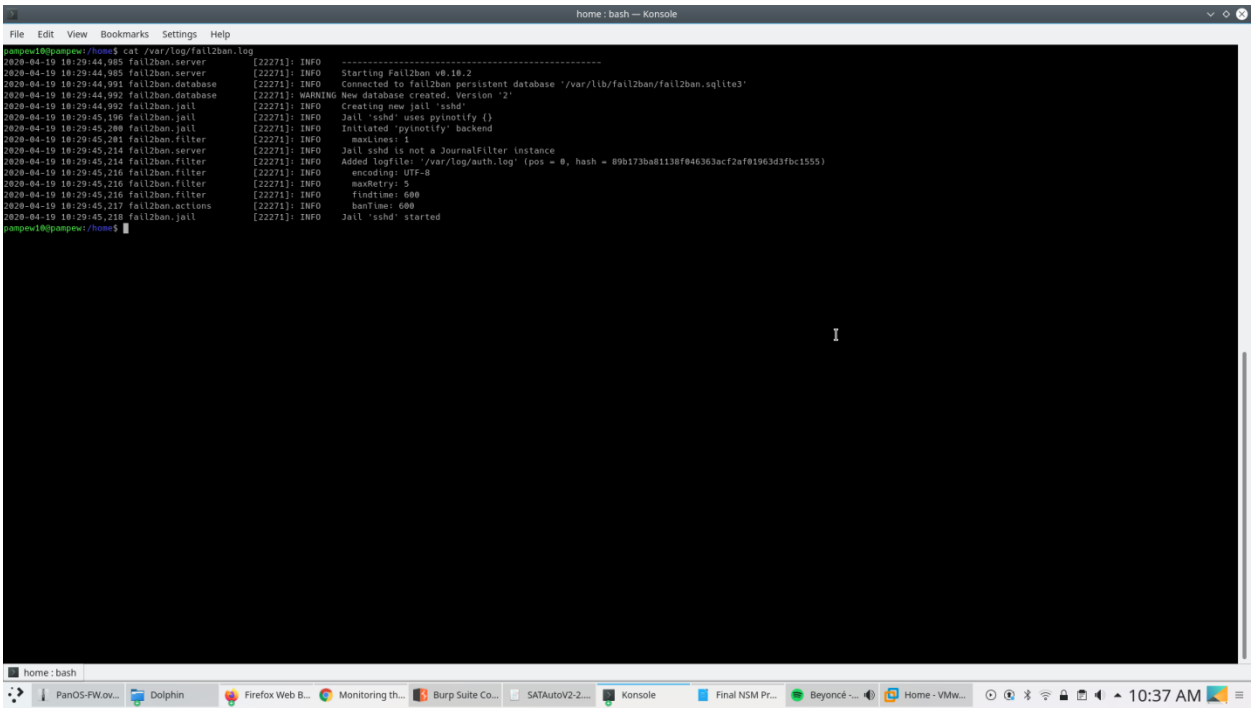
I wanted for my tool/s to go into more niche areas of network security monitoring tools that are by all technicality considered NSM tools but differ from some primarily regarded tools like those in security onion. I will be deploying both instances on my kubuntu distribution with my personal laptop. These tools do not perform the same actions in a sense as tools like Wireshark and other monitoring tools as fail2ban is a monitoring tool that detects openssh brute force attacks or whatever is defined by the user and burp suite is a tool that can be used to test web applications and specific traffic with the ability to edit that traffic.

Burp Suite is an awesome tool and can be used as a proxy to detect and change values for some web traffic. As you have seen in a previous assignment (Wireshark challenge) this tool can be used in conjunction and will result in similar data to Wireshark. Here is an example of a website that my father owns and gave me permission to view. I could find all sorts of interesting information from this website based on what I was receiving and sending like how post and get requests information how the website determines the ID for certain things etc. With Burp Suite you can also perform attacks with repeater and intruder and other tools included in Burp Suite. An example of this is if you pushed the login screen to a repeater or intruder and attempted a repeat login for different parameters (passwords and usernames) . You can also find more information about the website thing your observing through target. You can view addons to the website directories etc. Here is an example picture.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Status Length MIME type Title Comment Time reque...
http://www.opensourc... GET /licenses/mit-license.... HTML
Request Response
Raw Headers Hex
GET /licenses/mit-license.php HTTP/1.1
Host: www.opensource.org
Accept: */*
Accept-Language: en
Connection: close
Type a search term
0 matches
10:27 AM

The other tool I mentioned is a very useful NSM tool that should in my opinion be on every Linux distribution with SSH capabilities. This tool can be used to detect SSH connections and halter them based on parameters set by the user. Fail2ban also has logging capabilities and is useful if someone just wants to watch ssh connections and attempts along with the IP of the attempted intruder. Here is an example of my config and log file below that.




home : bash — Konsole
File Edit View Bookmarks Settings Help
pampew10@pampew:/home$ cat /var/log/fail2ban.log
2020-04-19 10:29:44,985 fail2ban.server [22271]: INFO --
2020-04-19 10:29:44,985 fail2ban.server [22271]: INFO Starting Fail2ban v0.10.2
2020-04-19 10:29:44,991 fail2ban.database [22271]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2020-04-19 10:29:44,992 fail2ban.database [22271]: WARNING New database created. Version '2'
2020-04-19 10:29:44,992 fail2ban.jail [22271]: INFO Creating new jail 'sshd'
2020-04-19 10:29:45,196 fail2ban.jail [22271]: INFO Jail 'sshd' uses pyinotify {}
2020-04-19 10:29:45,200 fail2ban.jail [22271]: INFO Initiated 'pyinotify' backend
2020-04-19 10:29:45,201 fail2ban.filter [22271]: INFO maxLines: 1
2020-04-19 10:29:45,214 fail2ban.server [22271]: INFO Jail sshd is not a JournalFilter instance
2020-04-19 10:29:45,214 fail2ban.filter [22271]: INFO Added logfile: '/var/log/auth.log' (pos = 0, hash = 89b173ba81138f046363acf2af01963d3fbc1555)
2020-04-19 10:29:45,216 fail2ban.filter [22271]: INFO encoding: UTF-8
2020-04-19 10:29:45,216 fail2ban.filter [22271]: INFO maxRetry: 5
2020-04-19 10:29:45,216 fail2ban.filter [22271]: INFO findtime: 600
2020-04-19 10:29:45,217 fail2ban.actions [22271]: INFO banTime: 600
2020-04-19 10:29:45,218 fail2ban.jail [22271]: INFO Jail 'sshd' started
pampew10@pampew:/home$
home : bash
PanOS-FW.ov... Dolphin Firefox Web B... Monitoring th... Burp Suite Co... SATAutoV2-2.... Konsole Final NSM Pr... Beyoncé -... Home - VMw...
10:37 AM