SSH Intrusion Detector
User Manual

Gary Khodayari and Yuri Elt
February 8th, 2022

Purpose

The purpose of the User Manual is to provide instruction for users to use the SSH Intrusion Detector program.

How to

Monitor System Authentication Logs

Access to var/log

Type “Tail -f /var/log/auth.log” to display fail and success login in real-time.

Run script

To run the script, type ./ next to the name of the script file.

Example - ./Examplenamescript.sh

G8keep3r - Add user to watchlist file.

Example - sudo ./g8keep3r.sh – add Test02

G8keep3r - remove user to watchlist file.

Example - sudo ./g8keep3r.sh – remove Test02

G9keep3r - view banned usernames in the watchlist file.

Example - cat watch.list

Install Iptables

Iptables come pre-installed in most Linux systems. Better to check to make sure they are in the system.

This command line will update and install iptables if you don’t have them in your Linux system.

sudo apt-get update

sudo apt-get install iptables

Check the status of current iptables

This command line will check the status of current iptables. You can see INPUT, FORWARD, OUTPUT are set as accept or drop and reject.

sudo iptables -L v

Check banned users on the base of iptables

This command line will allow you to check and view banned users from iptable

iptables -L INPUT -v -n

Set up Rules

Set up rules with -A will allow you to set a specific rule for INPUT, FORWARD, OUTPUT

sudo iptables -A

Allow specific IP

If you want to allow a specific IP address then enter this command line. xxx is a general example of an IP address.

iptables -A INPUT -s xxx.xxx.x.x -j ACCEPT

iptables -A OUTPUT -d xxx.xxx.x.x -j ACCEPT

iptables -P INPUT DROP

iptables -P OUTPUT DROP

Block specific IP

If you want to block a specific IP address then enter this command line. xxx is a general example of an IP address.

iptables -A INPUT -s xxx.xxx.x.x -j DROP

iptables -A OUTPUT -d xxx.xxx.x.x -j DROP

iptables -P INPUT DROP

iptables -P OUTPUT DROP

Save Rules After Reboot

If you want to save the change that you made for your firewall, run this command

service iptables save

Deleting Rules

To delete the existing rule, use this command line

sudo iptables -F

Stop program's running script.

To stop the program's running. Press the "c" key to stop the running.

Exit program

This command line will end the program and exit.

sudo exit

Delete all files in var/log

If you don't need any files in var/log, use this command line

Sudo find /var/log -type f -delete

Advised: you may no longer have access to those logs again after this point.