

SSH Intrusion Detector Testing

Gary Khodayari and Yuri Elt
February 8th, 2022

Test Results	3
Examples	
Run the script without adding a username	3
Add the username to the watchlist file	3
Remove the username from the watchlist file	3
Prevent the duplicate usernames	3
Show list of banned usernames	4
Show iptable banned the test user with localhost IP	4

Test Results

Run the script without adding a username.

```
test01x@test01x-VirtualBox:~/Desktop/Script Folder$ sudo ./g8keep3r.sh
this script requires a username as an argument
use --help to display this message
Correct Usage:
  g8keepr --add <username>
  g8keepr --remove <username>
test01x@test01x-VirtualBox:~/Desktop/Script Folder$
```

If the user runs the script without argument (username).

Add the username to the watchlist file.

```
test01x@test01x-VirtualBox:~/Desktop/Script Folder$ sudo ./g8keep3r.sh --add Test02
watching Test02
test01x@test01x-VirtualBox:~/Desktop/Script Folder$
```

If the user wants to manually add the username to the watchlist file.

Remove the username from the watchlist file.

```
test01x@test01x-VirtualBox:~/Desktop/Script Folder$ sudo ./g8keep3r.sh --remove Test02
removing Test02 from the watched list
```

If the user wants to manually remove the username from the watchlist file.

Prevent the duplicate usernames if there is an existing username in the watch file.

```
test01x@test01x-VirtualBox:~/Desktop/Script Folder/g8keep3r-master$ sudo ./g8keep3r.sh --add Test01
watching Test01
test01x@test01x-VirtualBox:~/Desktop/Script Folder/g8keep3r-master$ sudo ./g8keep3r.sh --add Test01
this username is already being watched for
to remove a user from the watchlist please use --remove <username>
test01x@test01x-VirtualBox:~/Desktop/Script Folder/g8keep3r-master$
```

This test shows that the user can't add the same username if it is already on the watchlist file.

Show list of banned usernames

```
test01x@test01x-VirtualBox:~/Desktop/g8keep3r-master$ cat watch.list
test01
Test01
Test02
Test03
Test04
Test05
```

Show iptable banned the test user with localhost IP

```
test01x@test01x-VirtualBox:~/Desktop/g8keep3r-master$ sudo iptables -L INPUT -v -n
Chain INPUT (policy ACCEPT 1196 packets, 393K bytes)
 pkts bytes target    prot opt in      out     source       destination
    0     0 DROP      all  --  *      *       0.0.0.0/0    0.0.0.0/0
        match-set g8keep3r src
```

Match-set g8keep3r src shows that the localhost user got banned due to the "watchlist" file.