

PASSWORD GUESSING MONITOR TESTING

COMP 8006

SPENSER LEE A00925785

THOMAS YU A00915638

Contents

Testing.....	3
Figure 1	5
Figure 2	6
Figure 3	7
Figure 4	8
Figure 5	9
Figure 6	10
Figure 7	11
Figure 8	12
Figure 9	13
Figure 10	14
Figure 11	15
Figure 12	16
Figure 13	17
Figure 14	18

Testing

#	DESCRIPTION	STEPS	EXPECTED RESULT	RESULT
1	IPS shows successful ssh connection	1. ssh to server running IPS	IP address, program, attempts, last update, and "connected" status shown	PASS – Fig. 1
2	IPS shows disconnected ssh connect	1. ssh to server running IPS 2. exit ssh from client	IP address, program, attempts, last update, and "Disconnected" status shown	PASS – Fig. 2
3	IPS shows failed ssh attempt(s)	1. ssh to server running IPS with an invalid password	IP address, program, attempts, last update, and "Failed Attempt" status shown with failed attempts	PASS – Fig. 3
4	IPS shows attempt reset status	1. ssh to server running IPS with an invalid password 2. wait for the attempt reset time	IP address, program, attempts, last update, and "Attempts Reset" status shown with failed attempts	PASS – Fig. 4
5	IPS shows IP blocked status	1. ssh to server running IPS with an invalid password over the number of permitted attempts	IP address, program, attempts, last update, and "IP Blocked" status shown with failed attempts	PASS – Fig. 5
6	IPS shows IP unblocked status	1. ssh to server running IPS with an invalid password over the number of permitted attempts 2. wait for the IP block duration	IP address, program, attempts, last update, and "IP Unblocked" status shown with failed attempts	PASS – Fig. 6
7	IPS blocks IP address after an exceeded number of ssh attempts have been made.	1. ssh to server running IPS with an invalid password multiple times	IP address, program, attempts, last update, and "IP Blocked" status shown The IP shows up under the ip_block user chain when listing iptables -L	PASS – Fig. 7
8	IPS resets login attempts after a reset time	1. ssh to server running IPS with an invalid password 2. wait for reset time	IP address, program, attempts, last update, and "Attempts Reset" shown Cat-ing the activity log file shows attempts at 0	PASS – Fig. 8

9	IPS resets IP block after a block duration	<ol style="list-style-type: none"> 1. ssh to server running IPS multiple times with invalid passwords 2. wait for block duration 	Able to attempt ssh login after being blocked.	PASS – Fig. 9
10	IPS Unblocks all IPs	<ol style="list-style-type: none"> 1. Click “Unblock All IPs” on the IPS 	IPS log is cleared The user chain ip_block is empty when listing iptables -L	PASS – Fig. 10
11	Stop IPS	<ol style="list-style-type: none"> 1. Click “Stop Log Monitor Daemon” on the IPS 	Daemon is not shown on system monitor	PASS – Fig. 11
12	Multiple ssh attempts for multiple clients are shown	<ol style="list-style-type: none"> 1. ssh to server running the IPS on multiple clients 	IP address, program, attempts, last update, and “IP Block Expired” shown	PASS – Fig. 12
13	IPS starts via cron tab	<ol style="list-style-type: none"> 1. write to cron tab for reboot with desired parameters 	Daemon running on reboot	PASS – Fig. 13
14	Slow scan password attempt	<ol style="list-style-type: none"> 1. ssh to server running IPS in spaced out attempts 	IP is still banned once exceeded permitted attempts	PASS – Fig. 14

Figure 1

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Connected	ssh	0	09:03:50 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 2

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Disconnected	ssh	0	09:04:03 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 3

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Failed Attempt	ssh	1	09:01:15 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 4

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Attempts Reset	ssh	0	08:57:12 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 5

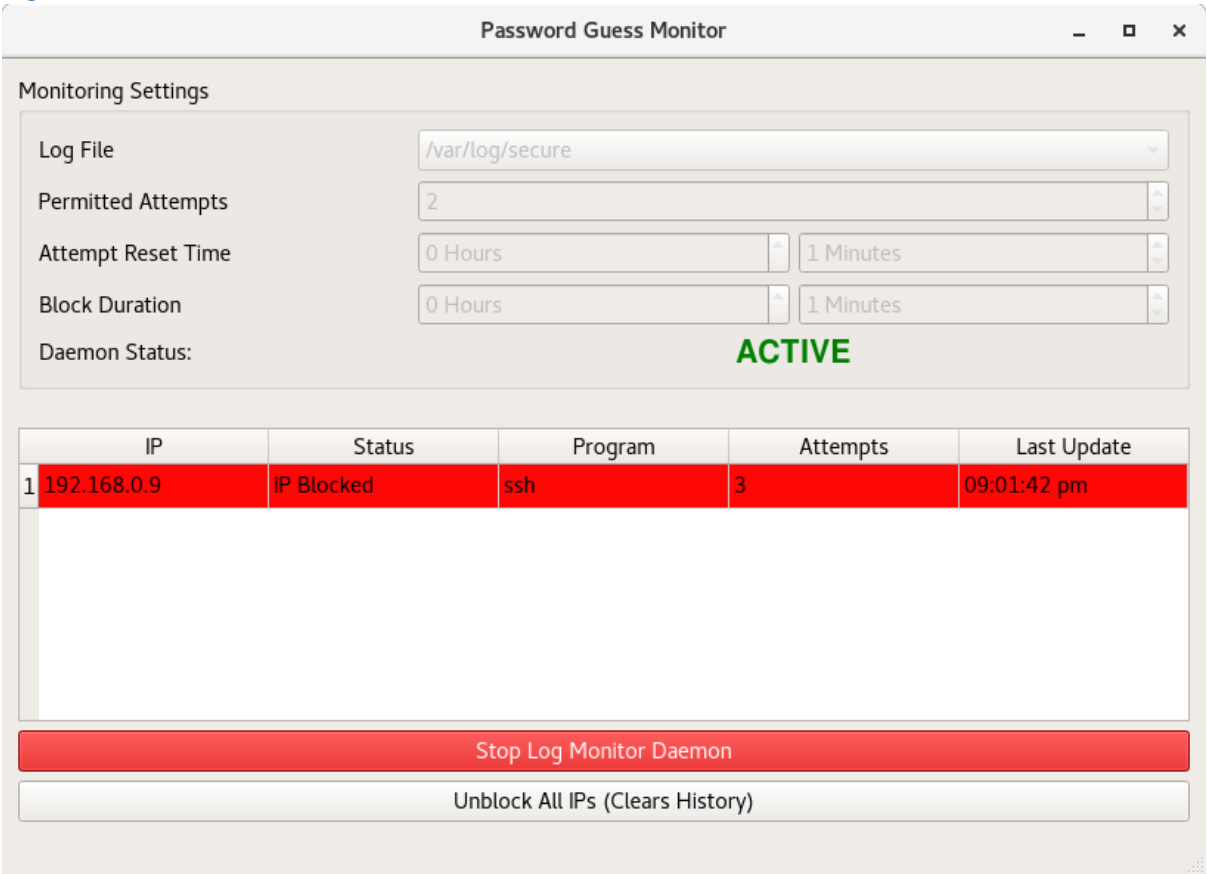


Figure 6

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	IP Block Expired	ssh	0	09:01:42 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 7

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	IP Blocked	ssh	3	09:01:42 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

```

Every 1.0s: iptables -L                               Wed Mar  8 21:02:15 2017

Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ip_block   all  --  anywhere              anywhere
ACCEPT     udp  --  anywhere              anywhere      udp dpt:domain
ACCEPT     tcp  --  anywhere              anywhere      tcp dpt:domain
ACCEPT     udp  --  anywhere              anywhere      udp dpt:bootps
ACCEPT     tcp  --  anywhere              anywhere      tcp dpt:bootps

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere              192.168.122.0/24    ctstate RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24      anywhere
ACCEPT     all  --  anywhere              anywhere
REJECT     all  --  anywhere              anywhere      reject-with icmp-port-unreachable
REJECT     all  --  anywhere              anywhere      reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     udp  --  anywhere              anywhere      udp dpt:bootpc

Chain ip_block (1 references)
target     prot opt source                destination
DROP       all  --  192.168.0.9           anywhere
  
```

Figure 8

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Attempts Reset	ssh	0	08:57:12 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

```
Every 1.0s: cat activity.log
{
  "login_attempts": [
    {
      "attempts": 0,
      "ip": "192.168.0.9",
      "program": "ssh",
      "status": "Attempts Reset",
      "time": "1489036159"
    }
  ]
}
```

Figure 9

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	IP Block Expired	ssh	0	09:01:42 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 10

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

IP	Status	Program	Attempts	Last Update
----	--------	---------	----------	-------------

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Chain ip_block (1 references)

target prot opt source destination

Figure 11

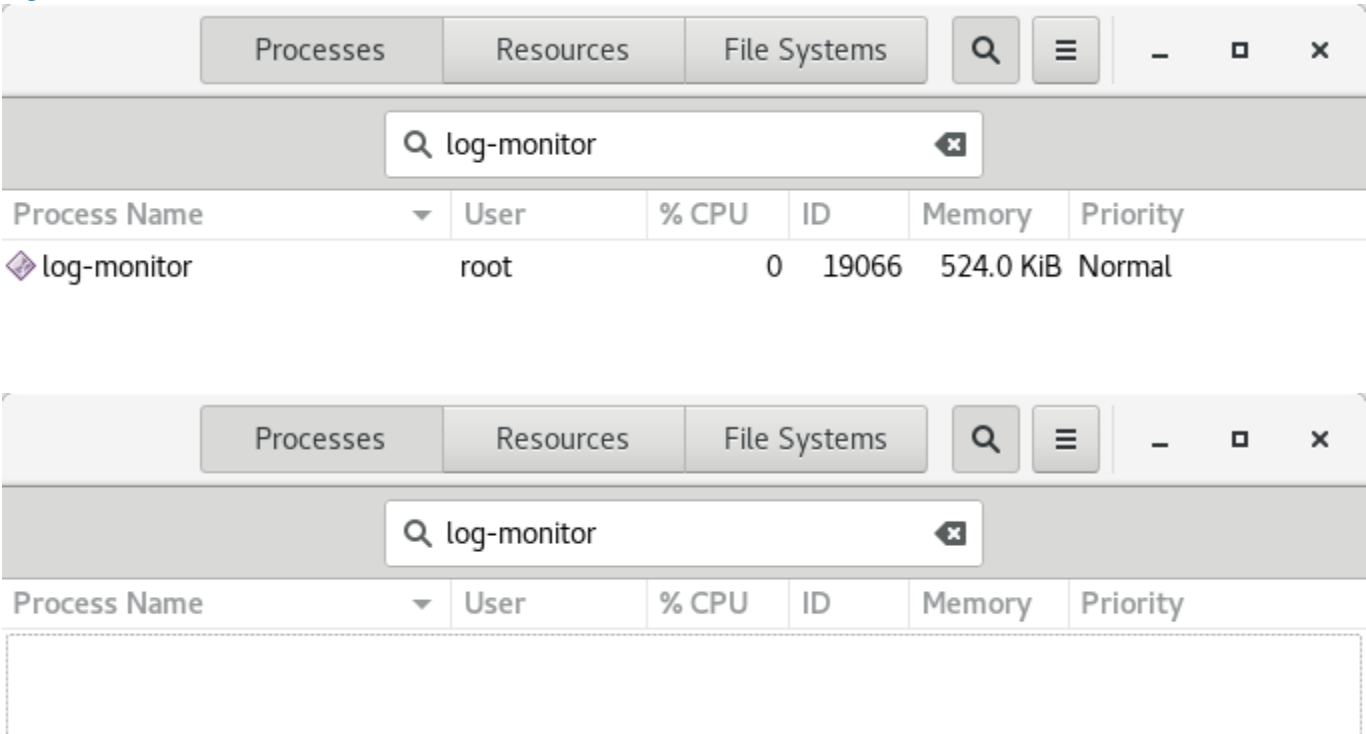


Figure 12

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

1

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	Attempts Reset	ssh	0	08:24:26 pm
2	192.168.0.6	Connected	ssh	1	08:26:18 pm
3	192.168.0.5	Failed Attempt	ssh	1	08:26:23 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)

Figure 13

The image shows two overlapping windows from a Linux system. The top window is a terminal titled 'root@datacomm:~' with a menu bar (File, Edit, View, Search, Terminal, Help). It shows the following commands and output:

```
[root@datacomm ~]# crontab -l
@reboot /root/Documents/log-monitor /var/log/secure 2 0 1 0 1
[root@datacomm ~]#
```

The bottom window is titled 'root@datacomm:~/Documents' and also has a menu bar. It shows the following commands and output:

```
[root@datacomm Documents]# ls
activity.log  log-monitor  log-monitor.pid  log-monitor.settings  pass
[root@datacomm Documents]# cat activity.log
{
  "login_attempts": [
    {
      "attempts": 1,
      "ip": "192.168.0.9",
      "program": "ssh",
      "status": "Failed Attempt",
      "time": "1489042609"
    }
  ]
}
[root@datacomm Documents]# uptime
22:56:54 up 1 min,  1 user,  load average: 0.51, 0.20, 0.07
[root@datacomm Documents]# crontab -l
@reboot /root/Documents/log-monitor /var/log/secure 2 0 1 0 1
[root@datacomm Documents]#
```

Overlaid on the right side of the bottom terminal window is a process monitor window. It has tabs for 'Processes', 'Resources', and 'Files'. A search bar contains 'log-mon'. Below the search bar is a table with two columns: 'Process Name' and 'User'.

Process Name	User
log-monitor	root

Figure 14

```
root@datacomm:~  
File Edit View Search Terminal Help  
[root@datacomm ~]# ssh 192.168.0.10  
root@192.168.0.10's password:  
Permission denied, please try again.  
root@192.168.0.10's password:  
Permission denied, please try again.  
root@192.168.0.10's password:  
  
[root@datacomm ~]# date  
Wed Mar 8 23:01:02 PST 2017  
[root@datacomm ~]# date  
Wed Mar 8 23:01:25 PST 2017  
[root@datacomm ~]# ssh 192.168.0.10  
root@192.168.0.10's password:  
Permission denied, please try again.  
root@192.168.0.10's password:  
  
[root@datacomm ~]#
```

Password Guess Monitor

Monitoring Settings

Log File

/var/log/secure

Permitted Attempts

2

Attempt Reset Time

0 Hours

1 Minutes

Block Duration

0 Hours

1 Minutes

Daemon Status:

ACTIVE

	IP	Status	Program	Attempts	Last Update
1	192.168.0.9	IP Blocked	ssh	3	11:01:31 pm

Stop Log Monitor Daemon

Unblock All IPs (Clears History)