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

1.1:

Step 5:

```
[sudo] password for sysadmin:
sysadmin@ubuntusrv:~$ service sshguard status
Osshguard.service - SSHGuard
    Loaded: loaded (/lib/systemd/system/sshguard.service; enabled; vendor presponder 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, staperocess: 1091 ExecStartPre=/usr/sbin/ip6tables -N sshguard (code=exited, staperocess: 1120 ExecStart=/usr/sbin/sshguard (code=killed, signal=TERM)
    Process: 4679 ExecStopPost=/usr/sbin/iptables -X sshguard (code=exited, staperocess: 4680 ExecStopPost=/usr/sbin/ip6tables -X sshguard (code=exited)
```

Step 8:

```
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:

1.2: Step 3:

```
sysadmin@ubuntusrv:~$ sudo cat /etc/sshquard/sshquard.conf
#### REQUIRED CONFIGURATION ####
# Full path to backend executable (required, no default)
BACKEND="/usr/lib/x86 64-linux-gnu/sshq-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 SYSL
OG 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:

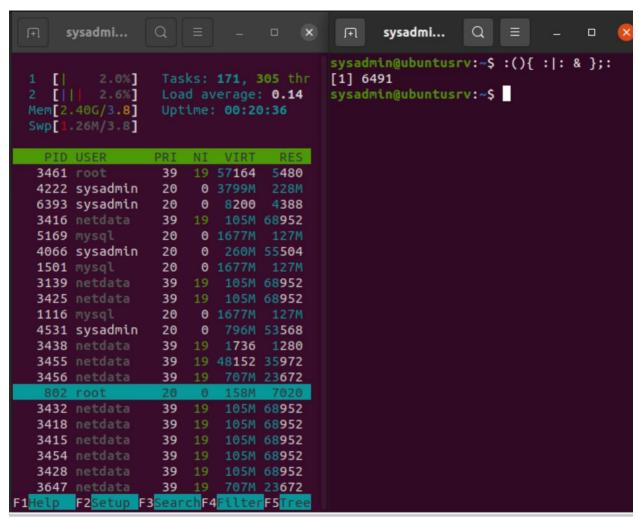
```
sshguard.service - SSHGuard
     Loaded: loaded (/lib/systemd/system/sshguard.service; enabled; vendor pres>
     Active: active (running) since Sat 2023-11-04 20:15:38 UTC; 46s ago
       Docs: man:sshguard(8)
    Process: 5728 ExecStartPre=/usr/sbin/iptables -N sshquard (code=exited, sta>
    Process: 5741 ExecStartPre=/usr/sbin/ip6tables -N sshquard (code=exited, st>
   Main PID: 5742 (sshquard)
      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
              —5746 /bin/sh /usr/sbin/sshguard
              -5748 /bin/journalctl -afb -p info -n1 -o cat SYSLOG_FACILITY=4 S>-5749 /bin/sh /usr/lib/x86_64-linux-gnu/sshg-fw-iptables
Nov 04 20:15:38 ubuntusrv.netlab.local sshquard[5757]: RETURN
                                                                     all -- 0.0.>
Nov 04 20:15:38 ubuntusrv.netlab.local sshquard[5757]: Chain DOCKER-ISOLATION-S
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: target
                                                                     prot opt sour>
Nov 04 20:15:38 ubuntusrv.netlab.local sshquard[5757]: DROP
                                                                     all -- 0.0.
Nov 04 20:15:38 ubuntusrv.netlab.local sshquard[5757]: RETURN
                                                                     all -- 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:
                                 IPv4 address for docker0: 172.17.0.1
 Memory usage: 64%
                                  IPv4 address for ens160: 172.16.1.10
 Swap usage:
 * 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
O 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:

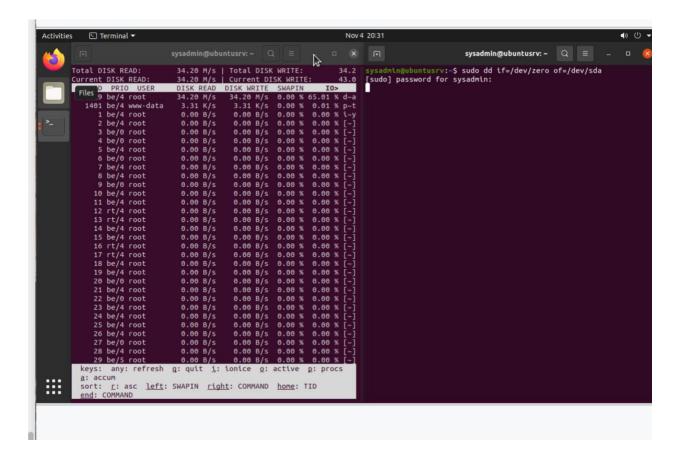
Step 5:



It froze ☺

3:

Step 7:



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.