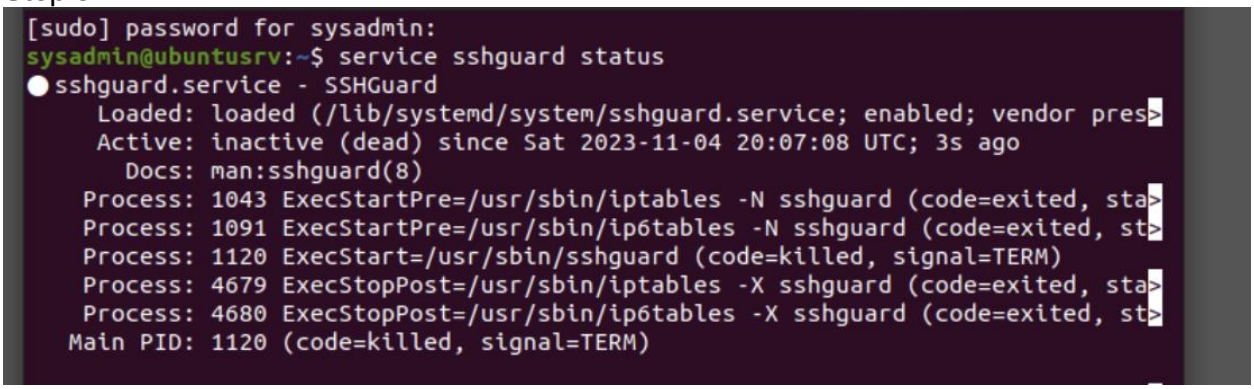
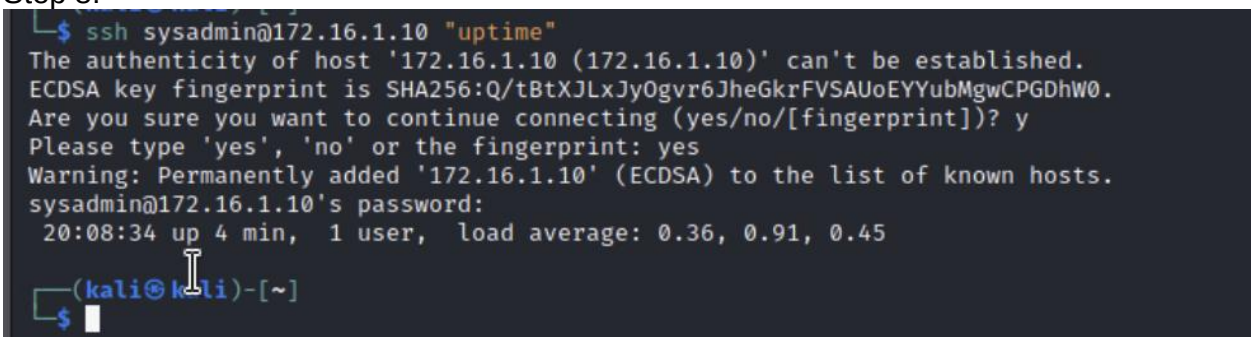
Peter Sanford
IT 2700
NetLab Lab 5
11/04/2023

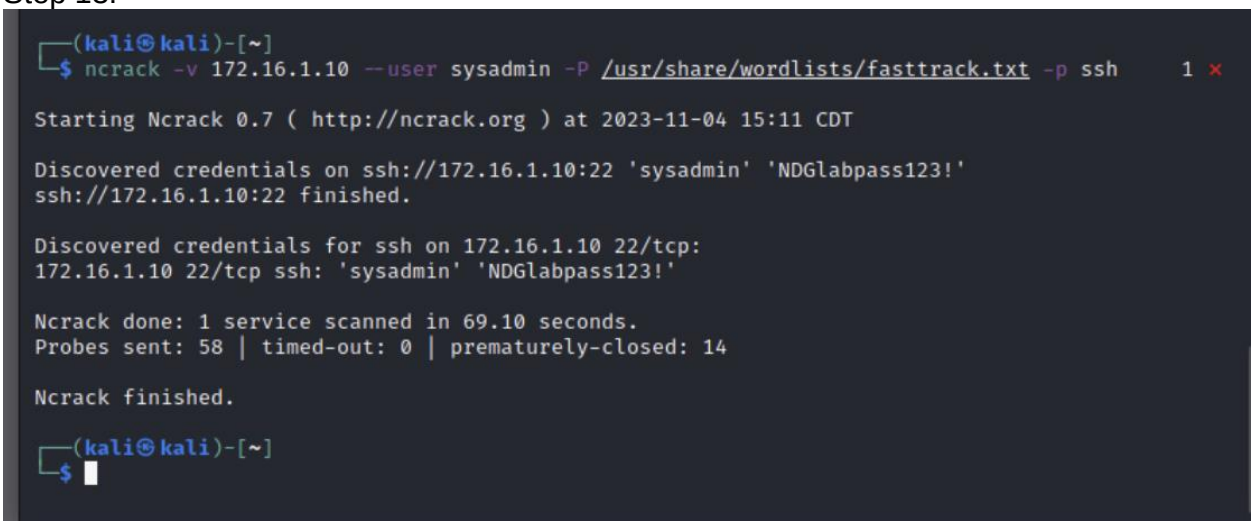
1.1:
Step 5:



Step 8:



Step 13:



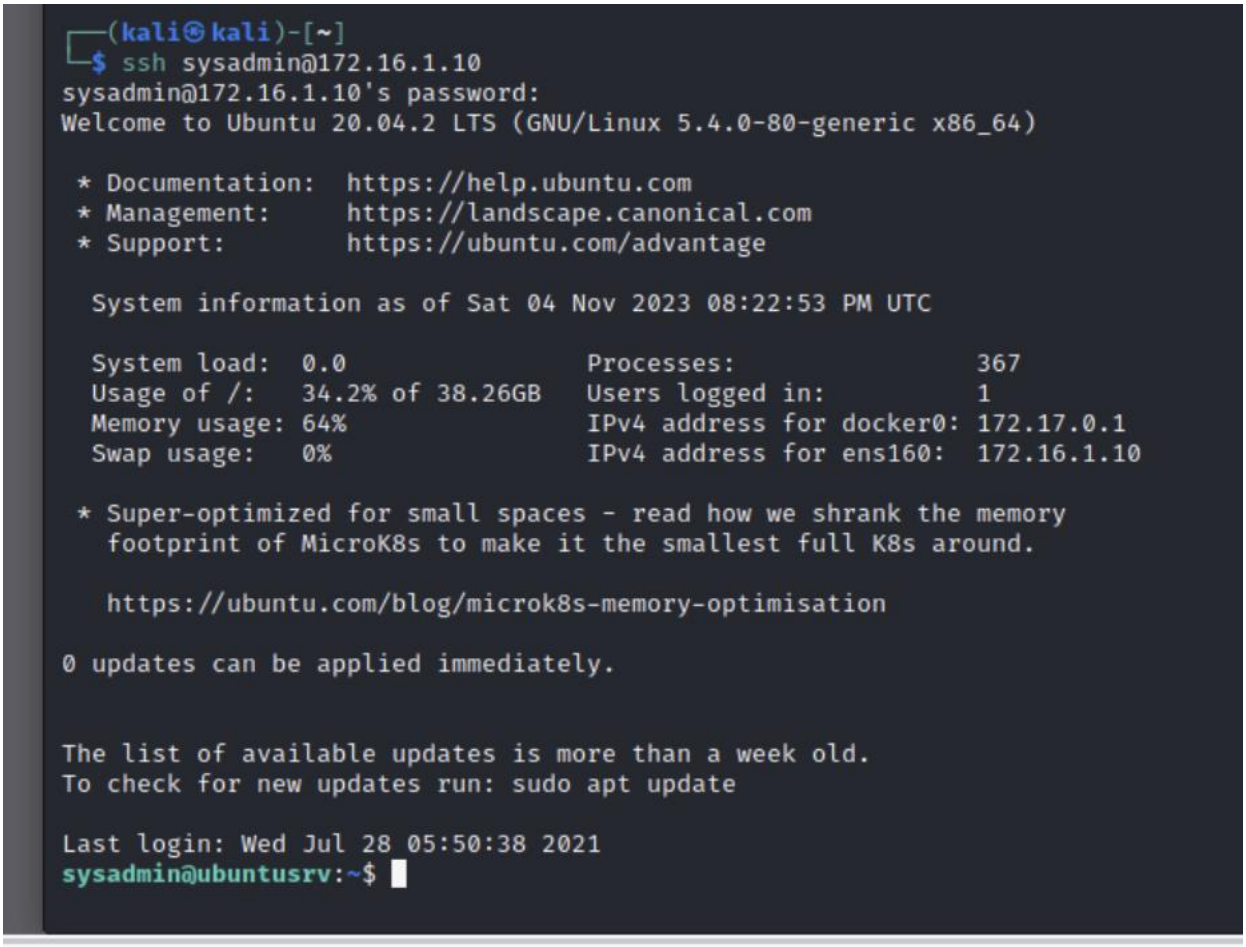
1.2:
Step 3:

```
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 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
```

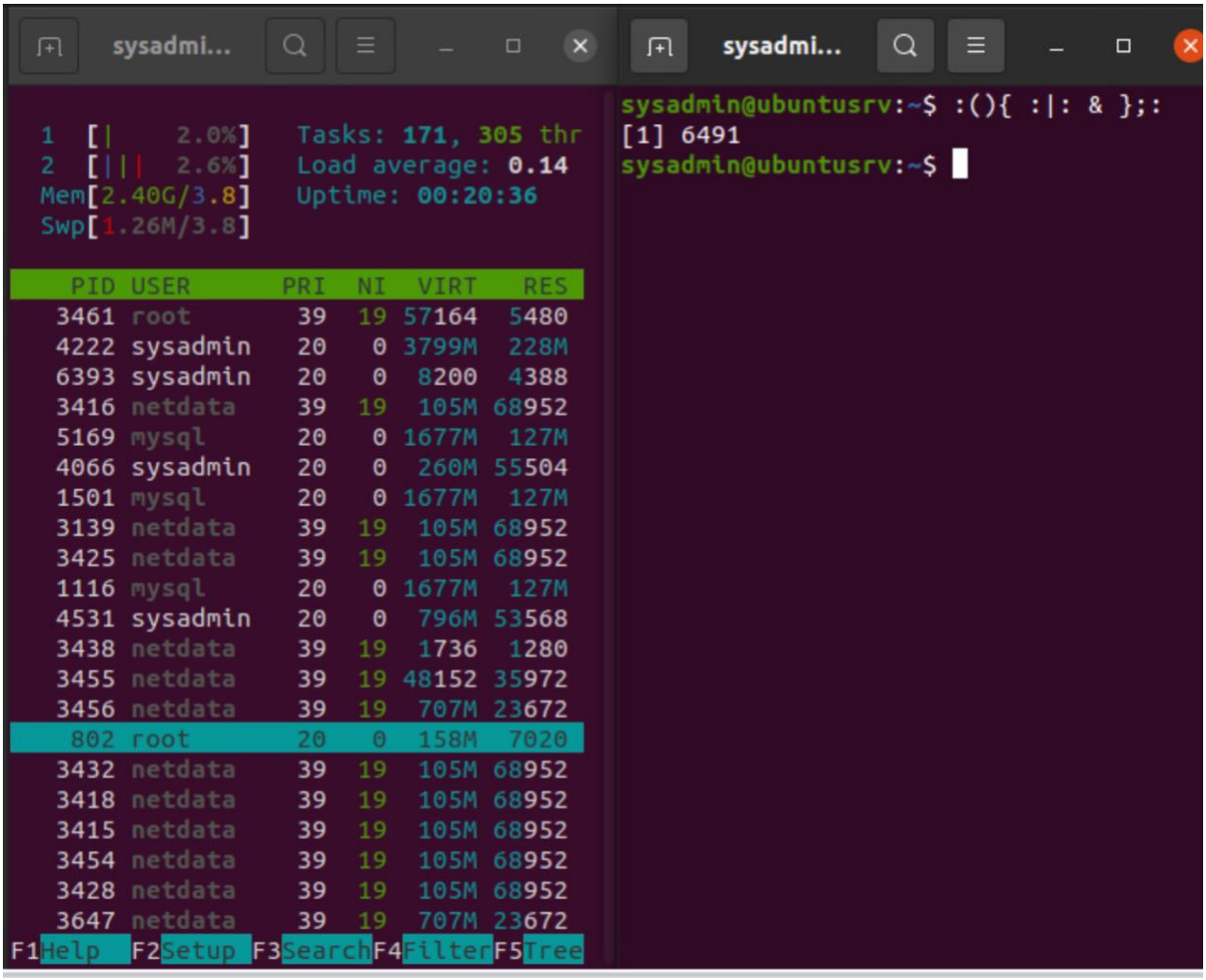
Step 5:

```
● 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 sshguard (code=exited, sta>
    Process: 5741 ExecStartPre=/usr/sbin/ip6tables -N sshguard (code=exited, st>
   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>
             ├─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 sshguard[5757]: RETURN     all  --  0.0.>
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[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 sshguard[5757]: DROP       all  --  0.0.>
Nov 04 20:15:38 ubuntusrv.netlab.local sshguard[5757]: RETURN     all  --  0.0.>
```

Step 10:

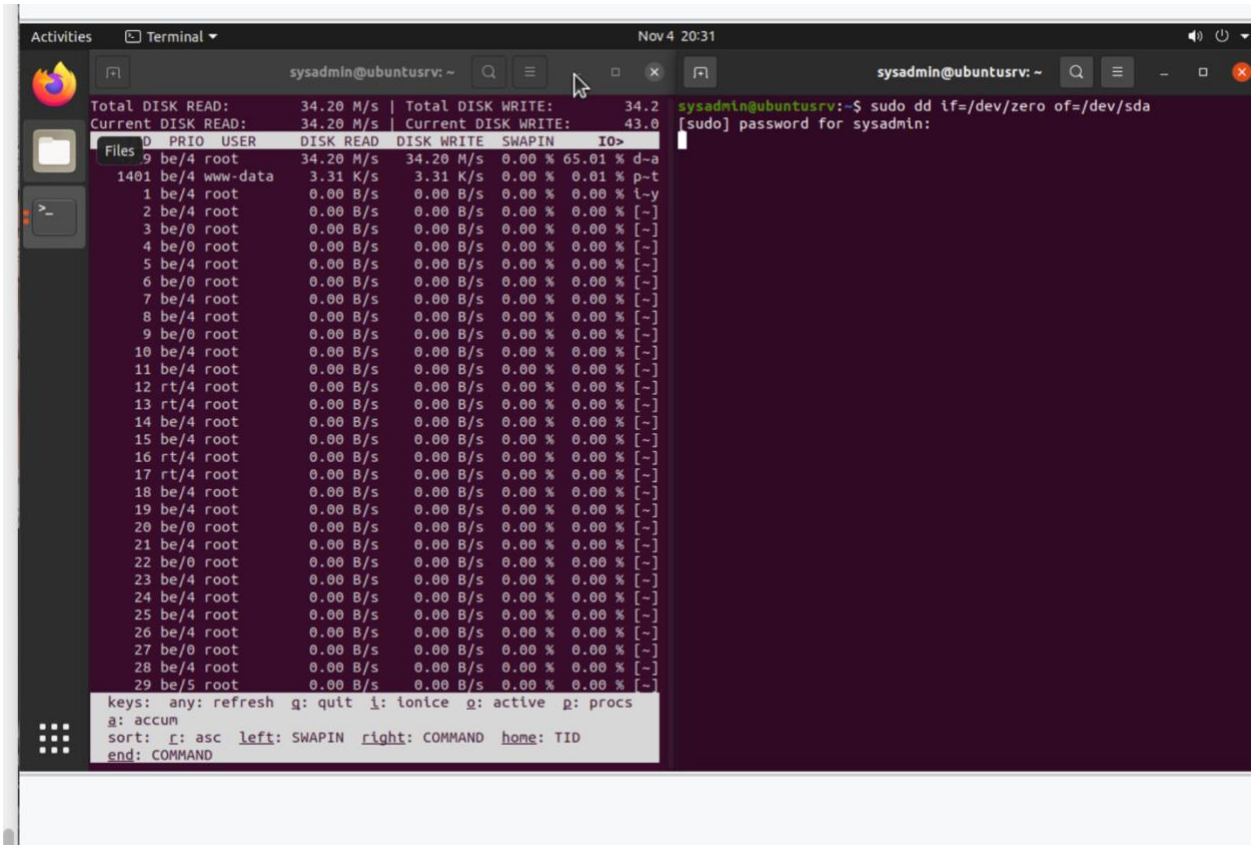

┌──(kali㉿kali)-[~]
└─$ ssh sysadmin@172.16.1.10
sysadmin@172.16.1.10's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Sat 04 Nov 2023 08:22:53 PM UTC
System load: 0.0
Usage of /: 34.2% of 38.26GB
Memory usage: 64%
Swap usage: 0%
Processes: 367
Users logged in: 1
IPv4 address for docker0: 172.17.0.1
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:



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.