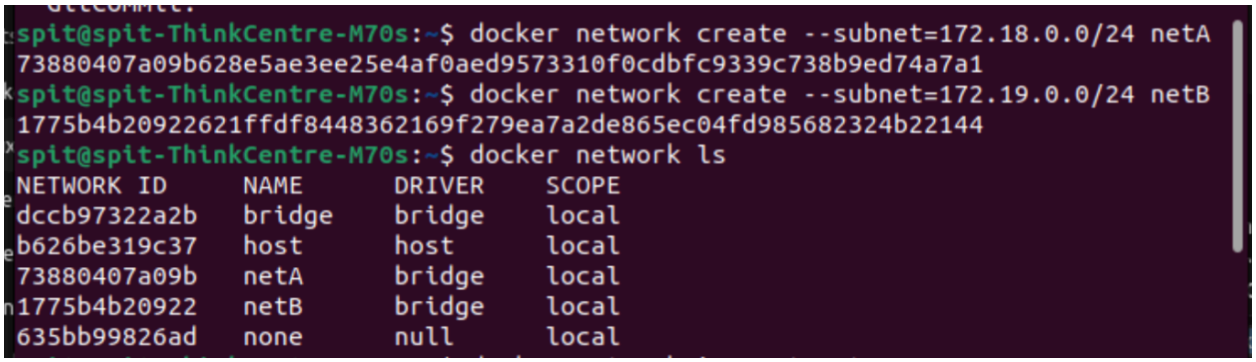


spit@spit-ThinkCentre-M70s:~$ docker network inspect netA


```
[
    {
        "Name": "netA",
        "Id": "73880407a09b628e5ae3ee25e4af0aed9573310f0cdbfc9339c738b9ed74a7a1",
        "Created": "2025-11-06T15:08:54.473293429+05:30",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv4": true,
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": {},
            "Config": [
                {
                    "Subnet": "172.18.0.0/24"
                }
            ]
        },
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {},
        "Options": {},
        "Labels": {}
    }
]
```

Firewall has both the containers

```
spit@spit-ThinkCentre-M70s:~$ docker inspect fw --format '{{json .NetworkSettings.Networks}}' |
python3 -m json.tool
{
    "netA": {
        "IPAMConfig": {
            "IPv4Address": "172.18.0.1"
        },
        "Links": null,
        "Aliases": [],
        "MacAddress": "",
        "DriverOpts": {},
        "GwPriority": 0,
        "NetworkID": "",
        "EndpointID": "",
        "Gateway": "",
        "IPAddress": "",
        "IPPrefixLen": 0,
        "IPv6Gateway": "",
        "GlobalIPv6Address": "",
        "GlobalIPv6PrefixLen": 0,
        "DNSNames": [
            "fw",
            "53a4db75cf80"
        ]
    },
    "netB": {
        "IPAMConfig": {
            "IPv4Address": "172.19.0.1"
        },
        "Links": null,
        "Aliases": [],
        "MacAddress": "",
        "DriverOpts": {},
        "GwPriority": 0,
        "NetworkID": "",
        "EndpointID": "",
        "Gateway": "",
        "IPAddress": "",
        "IPPrefixLen": 0,
        "IPv6Gateway": "",
```

```
        "GlobalIPv6Address": "",
        "GlobalIPv6PrefixLen": 0,
        "DNSNames": [
            "fw",
            "53a4db75cf80"
        ]
    }
}
spit@spit-ThinkCentre-M70s:~$
```


- `host1` = firewall machine (where you run iptables rules)
- `host2` = attacker/test machine
- Use a custom Docker bridge network so both containers have fixed IPs and can `ping` each other.
- To modify iptables and enable forwarding inside a container we run with capabilities (`--cap-add`) or `--privileged`.


```
spit@spit-ThinkCentre-M70s:~$ docker network inspect labnet | sed -n '1,120p'
[
    {
        "Name": "labnet",
        "Id": "db863790e650ab55bd8706d95d6eecb025812d77c5f273dbeb8cdfbfedd8b8a4",
        "Created": "2025-11-06T15:35:00.624111097+05:30",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv4": true,
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": {},
            "Config": [
                {
                    "Subnet": "192.168.56.0/24"
                }
            ]
        },
```

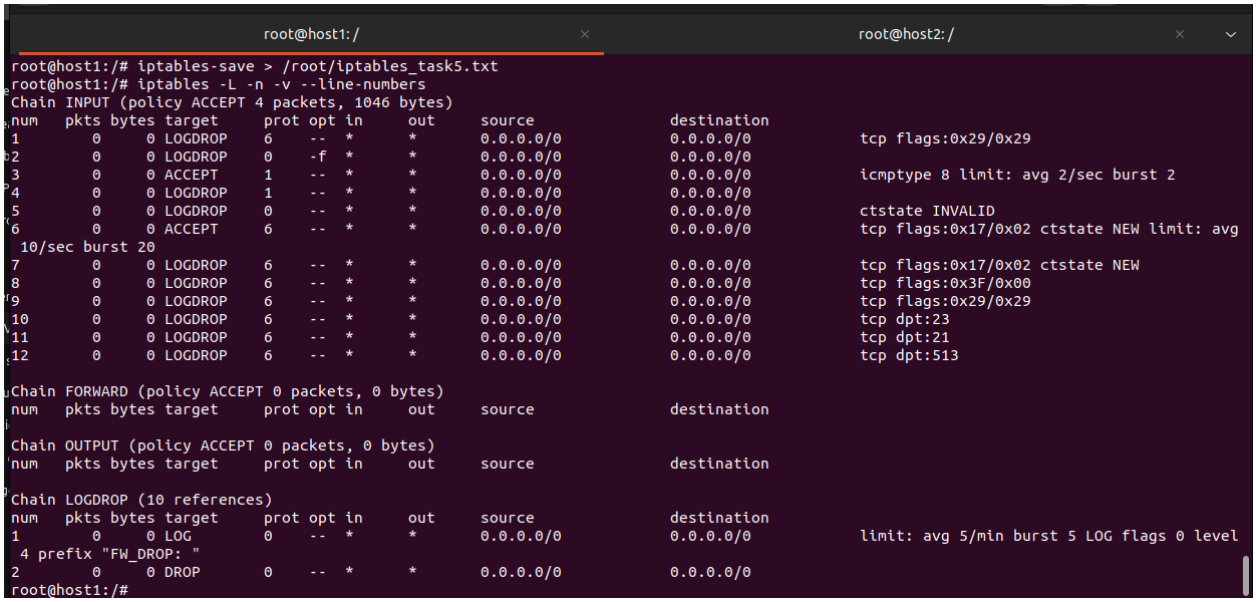
```
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {},
        "Options": {},
        "Labels": {}
    }
]
```

```
root@host1:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether ce:85:d8:21:0e:c6 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
       valid_lft forever preferred_lft forever
root@host1:/#
```

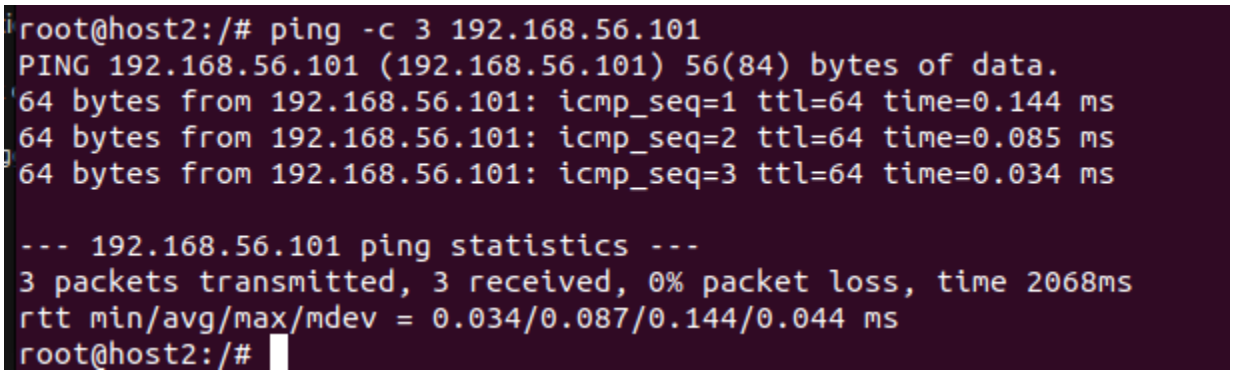
```
root@host2:/# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether ba:ce:0f:57:d9:17 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.56.102/24 brd 192.168.56.255 scope global eth0
       valid_lft forever preferred_lft forever
root@host2:/#
```

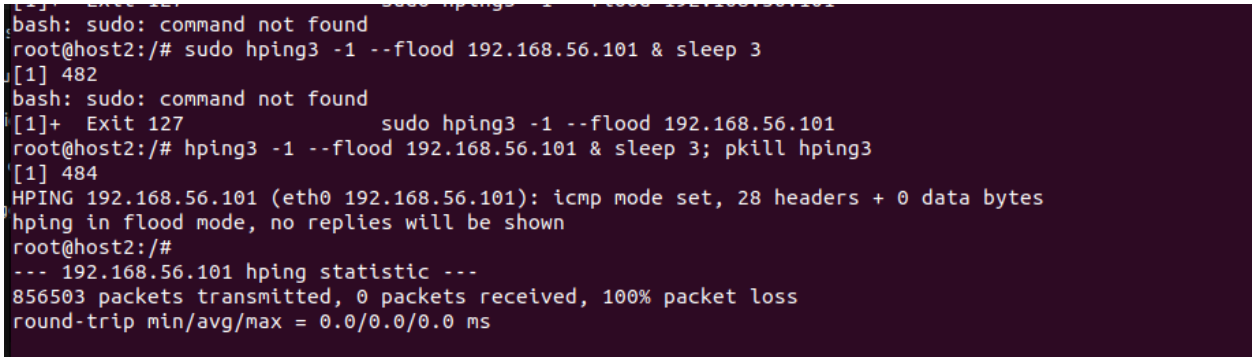
```
192.168.56.0/24 dev eth0 proto kernel scope link src 192.168.56.102
root@host2:/# ping -c 3 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.036 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.077 ms

--- 192.168.56.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.036/0.166/0.387/0.156 ms
root@host2:/# traceroute -n 192.168.56.101
traceroute to 192.168.56.101 (192.168.56.101), 30 hops max, 60 byte packets
 1  192.168.56.101  1.161 ms  1.031 ms  0.079 ms
root@host2:/#
```

```
root@host1:/# iptables-save > /root/iptables_before_tasks.txt
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 2 packets, 523 bytes)
num   pkts bytes target     prot opt in     out     source               destin
tion

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destin
tion

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destin
tion

Chain LOGDROP (0 references)
num   pkts bytes target     prot opt in     out     source               destin
tion
1        0     0 LOG        0    --  *      *       0.0.0.0/0            0.0.0.
/0           limit: avg 5/min burst 5 LOG flags 0 level 4 prefix "FW_DROP: "
2        0     0 DROP       0    --  *      *       0.0.0.0/0            0.0.0.
/0
root@host1:/#
```



Host2





FW_T1_COUNTERS
INPUT-4 : 856 000 packets, 24 M bytes
LOGDROP-1: 5 packets logged (140 B)
LOGDROP-2: 856 000 packets dropped (24 M bytes)
Chain INPUT (policy ACCEPT 4 packets, 1046 bytes)

```
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
3        0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8 limit: avg
2/sec burst 2
4        0     0 LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
5        0     0 LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate INVALID
6        0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02
ctstate NEW
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0            limit: avg 5/min burst 5
LOG flags 0 level 4 prefix "FW_DROP: "
2        0     0 DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 4 packets, 1046 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
3       10   448 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8 limit:
avg 2/sec burst 2
4      856K   24M LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
5        0     0 LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate INVALID
6        0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02
ctstate NEW
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23
```

```
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 10 packets, 448 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1        5   140 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst 5
LOG flags 0 level 4 prefix "FW_DROP: "
2      856K   24M DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/#
```

Task 2

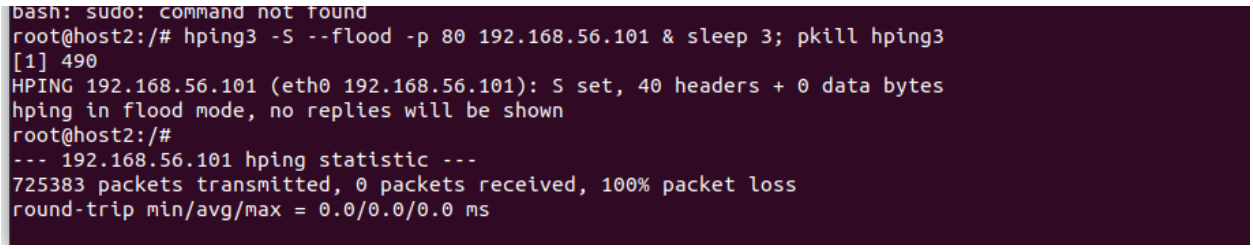
FW_T2_COUNTERS

INPUT-6 : 49 SYN packets accepted (1 960 B)

INPUT-7 : 725 k SYN packets dropped (29 M B)

LOGDROP-1: 10 packets logged (340 B)

LOGDROP-2: 1.58 M packets dropped (53 M B)




```
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 6 packets, 1569 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
3       10   448 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8 limit:
avg 2/sec burst 2
4      856K   24M LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
5        0     0 LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
6       49  1960 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7      725K   29M LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x17/0x02 ctstate NEW
```

```
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:23
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 59 packets, 2408 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1       10   340 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst 5
LOG flags 0 level 4 prefix "FW_DROP: "
2     1582K   53M DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/#
```

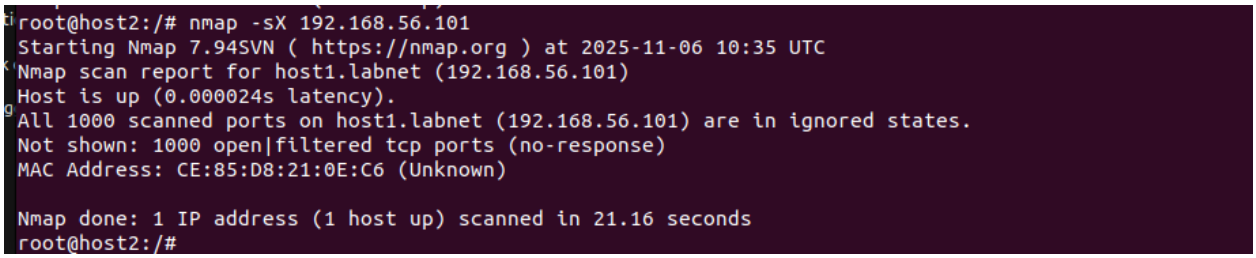
Task 3

```
root@host2:/# nmap -sN 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-06 10:32 UTC
Nmap scan report for host1.labnet (192.168.56.101)
Host is up (0.000024s latency).
All 1000 scanned ports on host1.labnet (192.168.56.101) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: CE:85:D8:21:0E:C6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.16 seconds
root@host2:/#
```

```
root@host2:/# nmap -sF 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-06 10:33 UTC
Nmap scan report for host1.labnet (192.168.56.101)
Host is up (0.000023s latency).
All 1000 scanned ports on host1.labnet (192.168.56.101) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: CE:85:D8:21:0E:C6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds
root@host2:/#
```

```
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 8 packets, 2092 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
3       10   448 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8 limit:
avg 2/sec burst 2
4     856K   24M LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
5     4000  160K LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
```

```
6       49  1960 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7     725K   29M LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x17/0x02 ctstate NEW
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:23
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 59 packets, 2408 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1       21   780 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst 5
LOG flags 0 level 4 prefix "FW_DROP: "
2     1586K   53M DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/#

FW_T3_COUNTERS
INPUT-5 : 4 000 packets, 160 k bytes (INVALID)
LOGDROP-1: 21 packets logged (780 B)
LOGDROP-2: 1.586 M packets dropped (53 M B)
```




```
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 8 packets, 2092 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1     2000 80000 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
3       10   448 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8 limit:
avg 2/sec burst 2
4     856K   24M LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
5     4000  160K LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
6       49  1960 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7     725K   29M LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x17/0x02 ctstate NEW
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:23
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 59 packets, 2408 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1       27  1020 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst
5 LOG flags 0 level 4 prefix "FW_DROP: "
2     1588K   53M DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/#
```

FW_T4_COUNTERS
INPUT-1 : 2 000 packets, 80 000 bytes (TCP XMAS flags 0x29/0x29)
LOGDROP-1: 27 packets logged (1 020 B)
LOGDROP-2: 1.588 M packets dropped (53 M B)

Task 5:

```
Host is up (0.000024s latency).
All 1000 scanned ports on host1.labnet (192.168.56.101) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: CE:85:D8:21:0E:C6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.16 seconds
root@host2:/# telnet 192.168.56.101 23
Trying 192.168.56.101...
telnet: Unable to connect to remote host: Connection refused
root@host2:/#
```

```
root@host1:/# iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 8 packets, 2092 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1     2000 80000 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x29/0x29
2        0     0 LOGDROP    0    -f  *      *       0.0.0.0/0            0.0.0.0/0
```

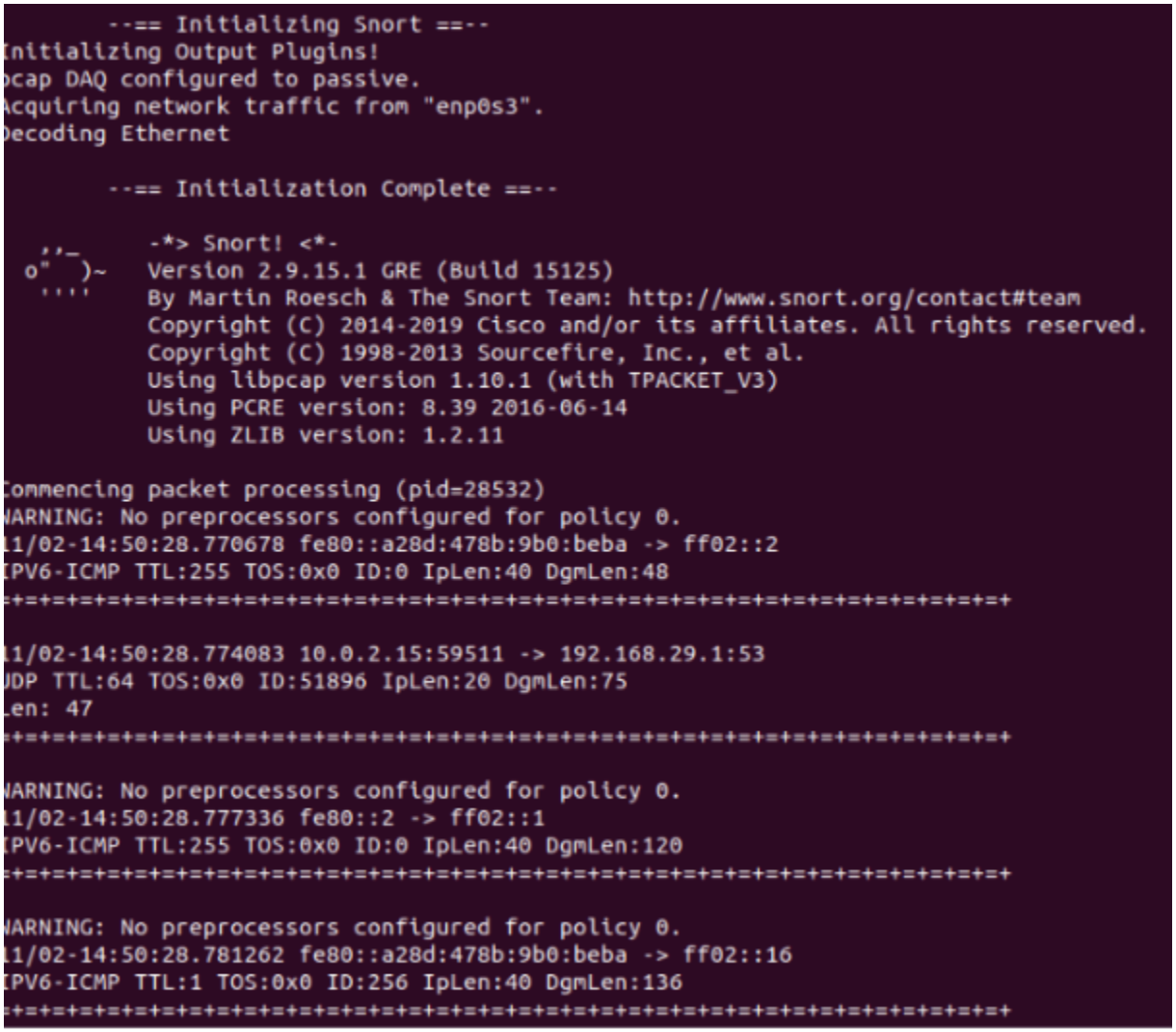
```
3       10   448 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8 limit:
avg 2/sec burst 2
4     856K   24M LOGDROP    1    --  *      *       0.0.0.0/0            0.0.0.0/0
5     4000  160K LOGDROP    0    --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
6       50  2020 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
ctstate NEW limit: avg 10/sec burst 20
7     725K   29M LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp
flags:0x17/0x02 ctstate NEW
8        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
9        0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
10       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:23
11       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
12       0     0 LOGDROP    6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 60 packets, 2448 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain LOGDROP (10 references)
num   pkts bytes target     prot opt in     out     source               destination
1       27  1020 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 5/min burst
5 LOG flags 0 level 4 prefix "FW_DROP: "
2     1588K   53M DROP       0    --  *      *       0.0.0.0/0            0.0.0.0/0
root@host1:/#


FW_T5_COUNTERS
INPUT-10 (telnet / dport 23) : 0 packets, 0 bytes
INPUT-11 (ftp / dport 21) : 0 packets, 0 bytes

root@host1:/# iptables-save > /root/iptables_final_$(date +%F).txt
root@host1:/# ls -l /root/iptables_*.txt
-rw-r--r-- 1 root root  571 Nov  6 10:16 /root/iptables_before_tasks.txt
-rw-r--r-- 1 root root 1343 Nov  6 10:39 /root/iptables_final_2025-11-06.txt
-rw-r--r-- 1 root root  710 Nov  6 10:18 /root/iptables_task1.txt
-rw-r--r-- 1 root root  987 Nov  6 10:19 /root/iptables_task2.txt
-rw-r--r-- 1 root root 1132 Nov  6 10:19 /root/iptables_task3.txt
-rw-r--r-- 1 root root 1202 Nov  6 10:19 /root/iptables_task4.txt
-rw-r--r-- 1 root root 1339 Nov  6 10:20 /root/iptables_task5.txt
root@host1:/# cat /root/iptables_final_$(date +%F).txt | sed -n '1,240p'
# Generated by iptables-save v1.8.10 (nf_tables) on Thu Nov  6 10:39:45 2025
*filter
```

```
:INPUT ACCEPT [8:2092]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [60:2448]
:LOGDROP - [0:0]
-A INPUT -p tcp -m tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j LOGDROP
-A INPUT -f -j LOGDROP
-A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 2/sec --limit-burst 2 -j ACCEPT
-A INPUT -p icmp -j LOGDROP
-A INPUT -m conntrack --ctstate INVALID -j LOGDROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -m limit
--limit 10/sec --limit-burst 20 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j
LOGDROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j LOGDROP
-A INPUT -p tcp -m tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j LOGDROP
-A INPUT -p tcp -m tcp --dport 23 -j LOGDROP
-A INPUT -p tcp -m tcp --dport 21 -j LOGDROP
-A INPUT -p tcp -m tcp --dport 513 -j LOGDROP
-A LOGDROP -m limit --limit 5/min -j LOG --log-prefix "FW_DROP: "
-A LOGDROP -j DROP
COMMIT
# Completed on Thu Nov  6 10:39:45 2025
# Generated by iptables-save v1.8.10 (nf_tables) on Thu Nov  6 10:39:45 2025
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:DOCKER_OUTPUT - [0:0]
:DOCKER_POSTROUTING - [0:0]
COMMIT
# Completed on Thu Nov  6 10:39:45 2025
```

```
~$ snort -V

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

~$
```

```
  GNU nano 6.2                    /etc/snort/snort.conf
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
File Name to Write: /etc/snort/snort.conf
^G Help          M-D DOS Format     M-A Append         M-B Backup File
^C Cancel        M-M Mac Format     M-P Prepend        ^T Browse
```

Network Intrusion Detection System using SNORT



```
WARNING: No preprocessors configured for policy 0.
11/02-14:50:32.213477 2620:2d:4000:1::96:80 -> fd17:625c:f037:2:de38:397e:d2a:c23e:60126
TCP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A***F Seq: 0x1D711CBB  Ack: 0xD9C45D06  Win: 0xFFFF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/02-14:50:32.213553 fd17:625c:f037:2:de38:397e:d2a:c23e:60126 -> 2620:2d:4000:1::96:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A**** Seq: 0xD9C45D06  Ack: 0x1D711CBB  Win: 0xFC67  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

11/02-14:50:32.213910 fd17:625c:f037:2:de38:397e:d2a:c23e:60126 -> 2620:2d:4000:1::96:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A***F Seq: 0xD9C45D06  Ack: 0x1D711CBC  Win: 0xFC66  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/02-14:50:32.214496 2620:2d:4000:1::96:80 -> fd17:625c:f037:2:de38:397e:d2a:c23e:60126
TCP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:60
***A**** Seq: 0x1D711CBC  Ack: 0xD9C45D07  Win: 0xFFFF  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/02-14:50:37.564693 fe80::2 -> ff02::1
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:120
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/02-14:50:37.919082 fe80::a28d:478b:9b0:beba -> ff02::16
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:136
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
11/02-14:50:38.860470 fe80::a28d:478b:9b0:beba -> ff02::16
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:136
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

^Z
[1]+  Stopped                 sudo snort -v -i enp0s3
```

```
       --== Initialization Complete ==--

          -*> Snort! <*-
  ,,_     Version 2.9.15.1 GRE (Build 15125)
 o"  )~   By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''   Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.10.1 (with TPACKET_V3)
          Using PCRE version: 8.39 2016-06-14
          Using ZLIB version: 1.2.11

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: appid  Version 1.1  <Build 5>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
```

Host based Intrusion Detection System using Logwatch:

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo systemctl status ssh --no-pager
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2025-10-29 15:56:50 IST; 1 day 22h ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 977 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1013 (sshd)
      Tasks: 1 (limit: 18869)
     Memory: 2.3M
     CGroup: /system.slice/ssh.service
             └─1013 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Oct 29 15:56:49 students-HP-280-G3-SFF-Business-PC systemd[1]: Starting OpenBSD Secure Shell server...
Oct 29 15:56:50 students-HP-280-G3-SFF-Business-PC sshd[1013]: Server listening on 0.0.0.0 port 22.
Oct 29 15:56:50 students-HP-280-G3-SFF-Business-PC sshd[1013]: Server listening on :: port 22.
Oct 29 15:56:50 students-HP-280-G3-SFF-Business-PC systemd[1]: Started OpenBSD Secure Shell server.
students@students-HP-280-G3-SFF-Business-PC:~$
students@students-HP-280-G3-SFF-Business-PC:~$ # restart to be safe
students@students-HP-280-G3-SFF-Business-PC:~$ sudo systemctl restart ssh
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
students@students-HP-280-G3-SFF-Business-PC:~$
students@students-HP-280-G3-SFF-Business-PC:~$ # enable root login and password auth (edit the file)
students@students-HP-280-G3-SFF-Business-PC:~$ sudo sed -i 's/^#\?PermitRootLogin.*/PermitRootLogin yes/' /etc/ssh/sshd_config
students@students-HP-280-G3-SFF-Business-PC:~$ sudo sed -i 's/^#\?PasswordAuthentication.*/PasswordAuthentication yes/' /etc/ssh/sshd_config
students@students-HP-280-G3-SFF-Business-PC:~$
students@students-HP-280-G3-SFF-Business-PC:~$ # restart ssh
students@students-HP-280-G3-SFF-Business-PC:~$ sudo systemctl restart ssh
students@students-HP-280-G3-SFF-Business-PC:~$ sudo tail -F /var/log/auth.log
Oct 31 14:49:21 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 14:49:21 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session closed for user root
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/systemctl res
tart ssh
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sshd[10022]: Received signal 15; terminating.
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sshd[12600]: Server listening on 0.0.0.0 port 22.
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sshd[12600]: Server listening on :: port 22.
Oct 31 14:49:22 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session closed for user root
Oct 31 14:49:38 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/tail -F /var/
log/auth.log
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ ssh invaliduser@10.10.71.61
The authenticity of host '10.10.71.61 (10.10.71.61)' can't be established.
ED25519 key fingerprint is SHA256:IKqPuZCPSoT/aKlUw5SmcDqRulRG4A9m0N+bwmVkhYQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.71.61' (ED25519) to the list of known hosts.
invaliduser@10.10.71.61's password:
Permission denied, please try again.
invaliduser@10.10.71.61's password:
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ ssh root@10.10.71.61
root@10.10.71.61's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

164 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 20.04 at
https://ubuntu.com/20-04

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ ssh students@10.10.71.61
students@10.10.71.61's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

164 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 20.04 at
https://ubuntu.com/20-04

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Sep 15 11:48:19 2025 from 10.10.71.61
students@students-HP-280-G3-SFF-Business-PC:~$
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ # basic sshd report to console
students@students-HP-280-G3-SFF-Business-PC:~$ sudo logwatch --service sshd --range today --print
Unknown option: print

Usage: /usr/sbin/logwatch [--detail <level>] [--logfile <name>] [--output <output_type>]
   [--format <format_type>] [--encode <encoding>] [--numeric]
   [--mailto <addr>] [--archives] [--range <range>] [--debug <level>]
   [--filename <filename>] [--help|--usage] [--version] [--service <name>]
   [--hostformat <host_format type>] [--hostlimit <host1,host2>] [--html_wrap <num_characters>]

--detail <level>: Report Detail Level - High, Med, Low or any #.
--logfile <name>: *Name of a logfile definition to report on.
--logdir <name>: Name of default directory where logs are stored.
--service <name>: *Name of a service definition to report on.
--output <output type>: Report Output - stdout [default], mail, file.
--format <formatting>: Report Format - text [default], html.
--encode <encoding>: Encoding to use - none [default], base64.
--mailto <addr>: Mail report to <addr>.
--archives: Use archived log files too.
--filename <filename>: Used to specify they filename to save to. --filename <filename> [Forces output to file].
--range <range>: Date range: Yesterday, Today, All, Help
                             where help will describe additional options
--numeric: Display addresses numerically rather than symbolically and numerically
          (saves  a  nameserver address-to-name lookup).
--debug <level>: Debug Level - High, Med, Low or any #.
--hostformat: Host Based Report Options - none [default], split, splitmail.
--hostlimit: Limit report to hostname - host1,host2.
--hostname: overwrites hostname
--html_wrap <num_characters>: Default is 80.
--version: Displays current version.
--help: This message.
--usage: Same as --help.
* = Switch can be specified multiple times...
```

```
students@students-HP-280-G3-SFF-Business-PC:~$
students@students-HP-280-G3-SFF-Business-PC:~$ # successful root login (search for 'Accepted')
students@students-HP-280-G3-SFF-Business-PC:~$ sudo grep -i "Accepted" /var/log/auth.log | tail -n 50
Oct 31 14:52:23 students-HP-280-G3-SFF-Business-PC sshd[12689]: Accepted password for root from 10.10.71.115 port 58946 ssh2
Oct 31 14:55:25 students-HP-280-G3-SFF-Business-PC sshd[13000]: Accepted password for students from 10.10.71.115 port 37308 ssh2
Oct 31 14:59:14 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/grep -i Accep
ted /var/log/auth.log
students@students-HP-280-G3-SFF-Business-PC:~$
students@students-HP-280-G3-SFF-Business-PC:~$ # attempts from the attacker's IP
students@students-HP-280-G3-SFF-Business-PC:~$ sudo grep "10.10.71.115" /var/log/auth.log | tail -n 100
Oct 31 14:51:01 students-HP-280-G3-SFF-Business-PC sshd[12671]: Invalid user invaliduser from 10.10.71.115 port 43674
Oct 31 14:51:09 students-HP-280-G3-SFF-Business-PC sshd[12671]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
= rhost=10.10.71.115
Oct 31 14:51:12 students-HP-280-G3-SFF-Business-PC sshd[12671]: Failed password for invalid user invaliduser from 10.10.71.115 port 43674 ssh2
Oct 31 14:51:28 students-HP-280-G3-SFF-Business-PC sshd[12671]: Connection closed by invalid user invaliduser 10.10.71.115 port 43674 [preauth]
Oct 31 14:51:42 students-HP-280-G3-SFF-Business-PC sshd[12681]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
= rhost=10.10.71.115  user=students
Oct 31 14:51:44 students-HP-280-G3-SFF-Business-PC sshd[12681]: Failed password for students from 10.10.71.115 port 52406 ssh2
Oct 31 14:51:55 students-HP-280-G3-SFF-Business-PC sshd[12681]: message repeated 2 times: [ Failed password for students from 10.10.71.115 port
 52406 ssh2]
Oct 31 14:51:56 students-HP-280-G3-SFF-Business-PC sshd[12681]: Connection closed by authenticating user students 10.10.71.115 port 52406 [prea
uth]
Oct 31 14:51:56 students-HP-280-G3-SFF-Business-PC sshd[12681]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=
10.10.71.115  user=students
Oct 31 14:52:23 students-HP-280-G3-SFF-Business-PC sshd[12689]: Accepted password for root from 10.10.71.115 port 58946 ssh2
Oct 31 14:54:48 students-HP-280-G3-SFF-Business-PC sshd[12689]: Received disconnect from 10.10.71.115 port 58946:11: disconnected by user
Oct 31 14:54:48 students-HP-280-G3-SFF-Business-PC sshd[12689]: Disconnected from user root 10.10.71.115 port 58946
Oct 31 14:55:02 students-HP-280-G3-SFF-Business-PC sshd[12995]: Invalid user spit from 10.10.71.115 port 37968
Oct 31 14:55:07 students-HP-280-G3-SFF-Business-PC sshd[12995]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
= rhost=10.10.71.115
Oct 31 14:55:09 students-HP-280-G3-SFF-Business-PC sshd[12995]: Failed password for invalid user spit from 10.10.71.115 port 37968 ssh2
Oct 31 14:55:15 students-HP-280-G3-SFF-Business-PC sshd[12995]: Connection closed by invalid user spit 10.10.71.115 port 37968 [preauth]
Oct 31 14:55:25 students-HP-280-G3-SFF-Business-PC sshd[13000]: Accepted password for students from 10.10.71.115 port 37308 ssh2
Oct 31 14:59:14 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/grep 10.10.71
.115 /var/log/auth.log
students@students-HP-280-G3-SFF-Business-PC:~$
```

Event Correlation Analysis (ECA):

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo apt-get install -y sec
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 libfwupdplugin1 libqt5help5 libqt5sql5 libqt5sql5-sqlite libqt5xml5 libsdl-ttf2.0-0 libxmlb1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sec
0 upgraded, 1 newly installed, 0 to remove and 42 not upgraded.
Need to get 121 kB of archives.
After this operation, 509 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 sec all 2.8.2-1 [121 kB]
Fetched 121 kB in 1s (187 kB/s)
Selecting previously unselected package sec.
(Reading database ... 225005 files and directories currently installed.)
Preparing to unpack .../archives/sec_2.8.2-1_all.deb ...
Unpacking sec (2.8.2-1) ...
Setting up sec (2.8.2-1) ...
Created symlink /etc/systemd/system/default.target.wants/sec.service → /lib/systemd/system/sec.service.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.24) ...
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo mkdir -p /etc/sec
students@students-HP-280-G3-SFF-Business-PC:~$ sudo tee /etc/sec/simple_rules.conf > /dev/null <<'EOF'
> # Rule 1: 3 failed SSH password attempts in 60s
> type=SingleWithThreshold
> ptype=RegExp
> pattern=Failed password for .*
> desc=SEC ALERT: Multiple SSH failed password attempts
> action=pipe logger -p auth.warning "SEC Alert: Multiple SSH failed attempts from %{1}"
> window=60
> threshold=3
>
> # Rule 2: 3 sudo authentication failures in 60s
> type=SingleWithThreshold
> ptype=RegExp
> pattern=authentication failure;.*sudo:
> desc=SEC ALERT: Multiple sudo authentication failures
> action=pipe logger -p auth.warning "SEC Alert: Multiple sudo auth failures from %{1}"
> window=60
> threshold=3
>
> # Rule 3: 2 successful root logins in 120s
> type=SingleWithThreshold
> ptype=RegExp
> pattern=Accepted password for root from ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)
> desc=SEC ALERT: Multiple root login successes
> action=pipe logger -p auth.warning "SEC Alert: Multiple root logins from %{1}"
> window=120
> threshold=2
> EOF
students@students-HP-280-G3-SFF-Business-PC:~$
```

```
tudents@students-HP-280-G3-SFF-Business-PC:~$ sudo sec -input=/var/log/auth.log -conf=/etc/sec/simple_rules.conf
EC (Simple Event Correlator) 2.8.2
eading configuration from /etc/sec/simple_rules.conf
ule in /etc/sec/simple_rules.conf at line 2: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
ule in /etc/sec/simple_rules.conf at line 2: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
ule in /etc/sec/simple_rules.conf at line 11: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
ule in /etc/sec/simple_rules.conf at line 11: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
ule in /etc/sec/simple_rules.conf at line 20: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
ule in /etc/sec/simple_rules.conf at line 20: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
o valid rules found in configuration file /etc/sec/simple_rules.conf
o --bufsize command line option or --bufsize=0, setting --bufsize to 1
pening input file /var/log/auth.log
nteractive process, SIGINT can't be used for changing the logging level
C
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo tail -F /var/log/auth.log
[sudo] password for students:
Oct 31 15:07:48 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session closed for user root
Oct 31 15:07:48 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/tee /etc/sec/
simple_rules.conf
Oct 31 15:07:48 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 15:07:48 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session closed for user root
Oct 31 15:07:54 students-HP-280-G3-SFF-Business-PC pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Oct 31 15:07:54 students-HP-280-G3-SFF-Business-PC pkexec[15597]: students: Executing command [USER=root] [TTY=unknown] [CWD=/home/students] [C
OMMAND=/usr/lib/update-notifier/package-system-locked]
Oct 31 15:08:20 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/1 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/sec -input=/v
ar/log/auth.log -conf=/etc/sec/simple_rules.conf
Oct 31 15:08:20 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 15:08:40 students-HP-280-G3-SFF-Business-PC sudo: students : TTY=pts/0 ; PWD=/home/students ; USER=root ; COMMAND=/usr/bin/tail -F /var/
log/auth.log
Oct 31 15:08:40 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 31 15:09:01 students-HP-280-G3-SFF-Business-PC CRON[15725]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 31 15:09:01 students-HP-280-G3-SFF-Business-PC CRON[15725]: pam_unix(cron:session): session closed for user root
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15741]: Accepted password for students from 10.10.71.115 port 37278 ssh2
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15741]: pam_unix(sshd:session): session opened for user students by (uid=0)
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 19 of user students.
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15798]: Received disconnect from 10.10.71.115 port 37278:11: disconnected by user
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15798]: Disconnected from user students 10.10.71.115 port 37278
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15741]: pam_unix(sshd:session): session closed for user students
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 19 logged out. Waiting for processes to exit.
Oct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 19.
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: Accepted password for students from 10.10.71.115 port 42990 ssh2
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: pam_unix(sshd:session): session opened for user students by (uid=0)
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 20 of user students.
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15855]: Received disconnect from 10.10.71.115 port 42990:11: disconnected by user
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15855]: Disconnected from user students 10.10.71.115 port 42990
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: pam_unix(sshd:session): session closed for user students
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 20 logged out. Waiting for processes to exit.
Oct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 20.
Oct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: Accepted password for students from 10.10.71.115 port 46220 ssh2
Oct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: pam_unix(sshd:session): session opened for user students by (uid=0)
```

```
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15741]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 19 of user students.
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15798]: Received disconnect from 10.10.71.115 port 37278:11: disconnected by user
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15798]: Disconnected from user students 10.10.71.115 port 37278
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC sshd[15741]: pam_unix(sshd:session): session closed for user students
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 19 logged out. Waiting for processes to exit.
ct 31 15:10:52 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 19.
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: Accepted password for students from 10.10.71.115 port 42990 ssh2
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 20 of user students.
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15855]: Received disconnect from 10.10.71.115 port 42990:11: disconnected by user
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15855]: Disconnected from user students 10.10.71.115 port 42990
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 20 logged out. Waiting for processes to exit.
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 20.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: Accepted password for students from 10.10.71.115 port 46220 ssh2
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 21 of user students.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15916]: Received disconnect from 10.10.71.115 port 46220:11: disconnected by user
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15916]: Disconnected from user students 10.10.71.115 port 46220
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 21 logged out. Waiting for processes to exit.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 21.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: Accepted password for students from 10.10.71.115 port 34414 ssh2
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 22 of user students.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15972]: Received disconnect from 10.10.71.115 port 34414:11: disconnected by user
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15972]: Disconnected from user students 10.10.71.115 port 34414
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 22 logged out. Waiting for processes to exit.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 22.
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[15974]: Accepted password for students from 10.10.71.115 port 34416 ssh2
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[15974]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 23 of user students.
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[16036]: Received disconnect from 10.10.71.115 port 34416:11: disconnected by user
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[16036]: Disconnected from user students 10.10.71.115 port 34416
```

```
students@students-HP-280-G3-SFF-Business-PC: ~                    students@students-HP-280-G3-SFF-Business-PC: ~
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC sshd[15802]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 20 logged out. Waiting for processes to exit.
ct 31 15:11:03 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 20.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: Accepted password for students from 10.10.71.115 port 46220 ssh2
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 21 of user students.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15916]: Received disconnect from 10.10.71.115 port 46220:11: disconnected by user
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15916]: Disconnected from user students 10.10.71.115 port 46220
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC sshd[15862]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 21 logged out. Waiting for processes to exit.
ct 31 15:11:12 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 21.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: Accepted password for students from 10.10.71.115 port 34414 ssh2
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 22 of user students.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15972]: Received disconnect from 10.10.71.115 port 34414:11: disconnected by user
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15972]: Disconnected from user students 10.10.71.115 port 34414
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC sshd[15919]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 22 logged out. Waiting for processes to exit.
ct 31 15:11:20 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 22.
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[15974]: Accepted password for students from 10.10.71.115 port 34416 ssh2
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[15974]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 23 of user students.
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[16036]: Received disconnect from 10.10.71.115 port 34416:11: disconnected by user
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[16036]: Disconnected from user students 10.10.71.115 port 34416
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC sshd[15974]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 23 logged out. Waiting for processes to exit.
ct 31 15:11:28 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 23.
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC sshd[16061]: Accepted password for students from 10.10.71.115 port 33400 ssh2
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC sshd[16061]: pam_unix(sshd:session): session opened for user students by (uid=0)
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: New session 24 of user students.
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC sshd[16114]: Received disconnect from 10.10.71.115 port 33400:11: disconnected by user
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC sshd[16114]: Disconnected from user students 10.10.71.115 port 33400
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC sshd[16061]: pam_unix(sshd:session): session closed for user students
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 24 logged out. Waiting for processes to exit.
ct 31 15:11:35 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 24.
```

```
  ; COMMAND=/usr/bin/ls
 Oct 31 15:13:18 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty= ruser=stude
 nts rhost=  user=students
 Oct 31 15:13:20 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): conversation failed
 Oct 31 15:13:20 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): auth could not identify password for [students]
 Oct 31 15:13:20 students-HP-280-G3-SFF-Business-PC sudo: students : 1 incorrect password attempt ; TTY=unknown ; PWD=/home/students ; USER=root
  ; COMMAND=/usr/bin/ls
 Oct 31 15:13:23 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty= ruser=stude
 nts rhost=  user=students
 Oct 31 15:13:25 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): conversation failed
 Oct 31 15:13:25 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): auth could not identify password for [students]
 Oct 31 15:13:25 students-HP-280-G3-SFF-Business-PC sudo: students : 1 incorrect password attempt ; TTY=unknown ; PWD=/home/students ; USER=root
  ; COMMAND=/usr/bin/ls
 Oct 31 15:13:28 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty= ruser=stude
 nts rhost=  user=students
 Oct 31 15:13:29 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): conversation failed
 Oct 31 15:13:29 students-HP-280-G3-SFF-Business-PC sudo: pam_unix(sudo:auth): auth could not identify password for [students]
 Oct 31 15:13:29 students-HP-280-G3-SFF-Business-PC sudo: students : 1 incorrect password attempt ; TTY=unknown ; PWD=/home/students ; USER=root
  ; COMMAND=/usr/bin/ls
 Oct 31 15:13:32 students-HP-280-G3-SFF-Business-PC sshd[16210]: Received disconnect from 10.10.71.115 port 48336:11: disconnected by user
 Oct 31 15:13:32 students-HP-280-G3-SFF-Business-PC sshd[16210]: Disconnected from user students 10.10.71.115 port 48336
 Oct 31 15:13:32 students-HP-280-G3-SFF-Business-PC sshd[16156]: pam_unix(sshd:session): session closed for user students
 Oct 31 15:13:32 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Session 25 logged out. Waiting for processes to exit.
 Oct 31 15:13:32 students-HP-280-G3-SFF-Business-PC systemd-logind[874]: Removed session 25.
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo apt-get install sec
[sudo] password for students:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sec
0 upgraded, 1 newly installed, 0 to remove and 245 not upgraded.
Need to get 129 kB of archives.
After this operation, 549 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 sec all 2.9.2-1 [129 kB]
Fetched 129 kB in 1s (118 kB/s)
Selecting previously unselected package sec.
(Reading database ... 348391 files and directories currently installed.)
Preparing to unpack .../archives/sec_2.9.2-1_all.deb ...
Unpacking sec (2.9.2-1) ...
Setting up sec (2.9.2-1) ...
Created symlink /etc/systemd/system/default.target.wants/sec.service → /usr/lib/systemd/system/sec.service.
Processing triggers for man-db (2.12.0-4build2) ...
students@students-HP-280-G3-SFF-Business-PC:~$
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ ping -c 3 10.10.71.61
PING 10.10.71.61 (10.10.71.61) 56(84) bytes of data.
64 bytes from 10.10.71.61: icmp_seq=1 ttl=64 time=0.551 ms
64 bytes from 10.10.71.61: icmp_seq=2 ttl=64 time=0.598 ms
64 bytes from 10.10.71.61: icmp_seq=3 ttl=64 time=0.549 ms

--- 10.10.71.61 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.549/0.566/0.598/0.022 ms
students@students-HP-280-G3-SFF-Business-PC:~$
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ for i in {1..6}; do
> ssh -o StrictHostKeyChecking=no students@10.10.71.61 exit || true
> sleep 5
> done
students@10.10.71.61's password:
students@10.10.71.61's password:
students@10.10.71.61's password:
students@10.10.71.61's password:
students@10.10.71.61's password:
students@10.10.71.61's password:
students@students-HP-280-G3-SFF-Business-PC:~$
```

```
students@students-HP-280-G3-SFF-Business-PC:~$ sudo sec -input=/var/log/auth.log -conf=/etc/sec/simple_rules.conf
SEC (Simple Event Correlator) 2.8.2
Reading configuration from /etc/sec/simple_rules.conf
Rule in /etc/sec/simple_rules.conf at line 2: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
Rule in /etc/sec/simple_rules.conf at line 2: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
Rule in /etc/sec/simple_rules.conf at line 11: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
Rule in /etc/sec/simple_rules.conf at line 11: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
Rule in /etc/sec/simple_rules.conf at line 20: Keyword 'thresh' missing (needed for SINGLEWITHTHRESHOLD rule)
Rule in /etc/sec/simple_rules.conf at line 20: Keyword 'threshold' illegal (not allowed for SINGLEWITHTHRESHOLD rule)
No valid rules found in configuration file /etc/sec/simple_rules.conf
No --bufsize command line option or --bufsize=0, setting --bufsize to 1
Opening input file /var/log/auth.log
Interactive process, SIGINT can't be used for changing the logging level
^C
```