Bhartiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to the University of Mumbai)
Academic Year: 2024 -25

Experiment No. 9

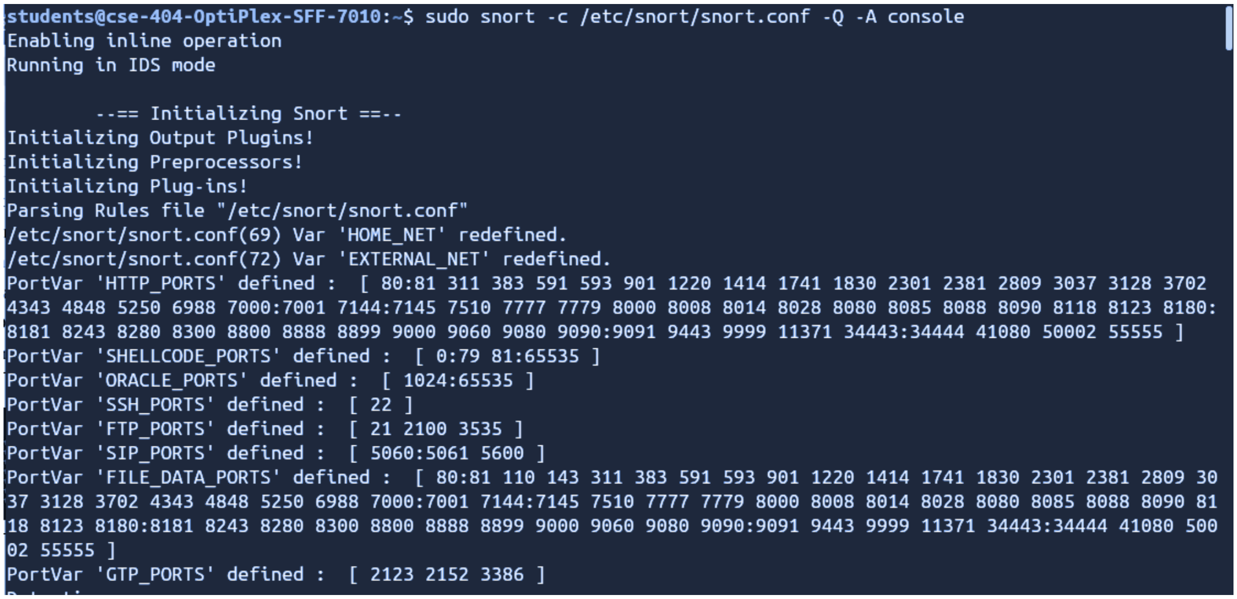
Semester: V **Batch:** A4

Name	Saayna Narvekar
Class	TE CSE – A4
UID	2023800067
Subject	Cryptography and Network Security

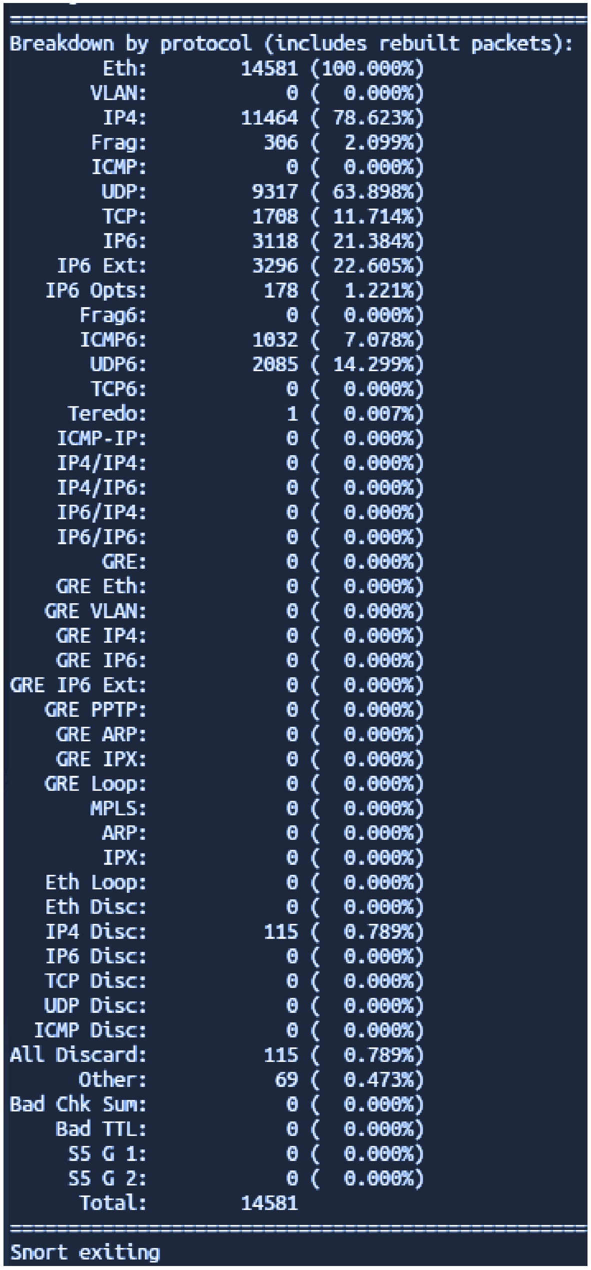
Aim: To implement i) Network Intrusion Detection System using SNORT:, ii)Host based Intrusion Detection System using Logwatch iii) Event Correlation Analysis (ECA) and iv) Building a Professional Firewall with Linux and Iptables andWindows Firewall

Problem Statement: An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. There are two main types of IDS:Network intrusion detection system (NIDS): It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders.Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of aNIDS is Snort.Host-based intrusion detection system (HIDS): It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access controllists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. An example of a HIDS is OSSEC.

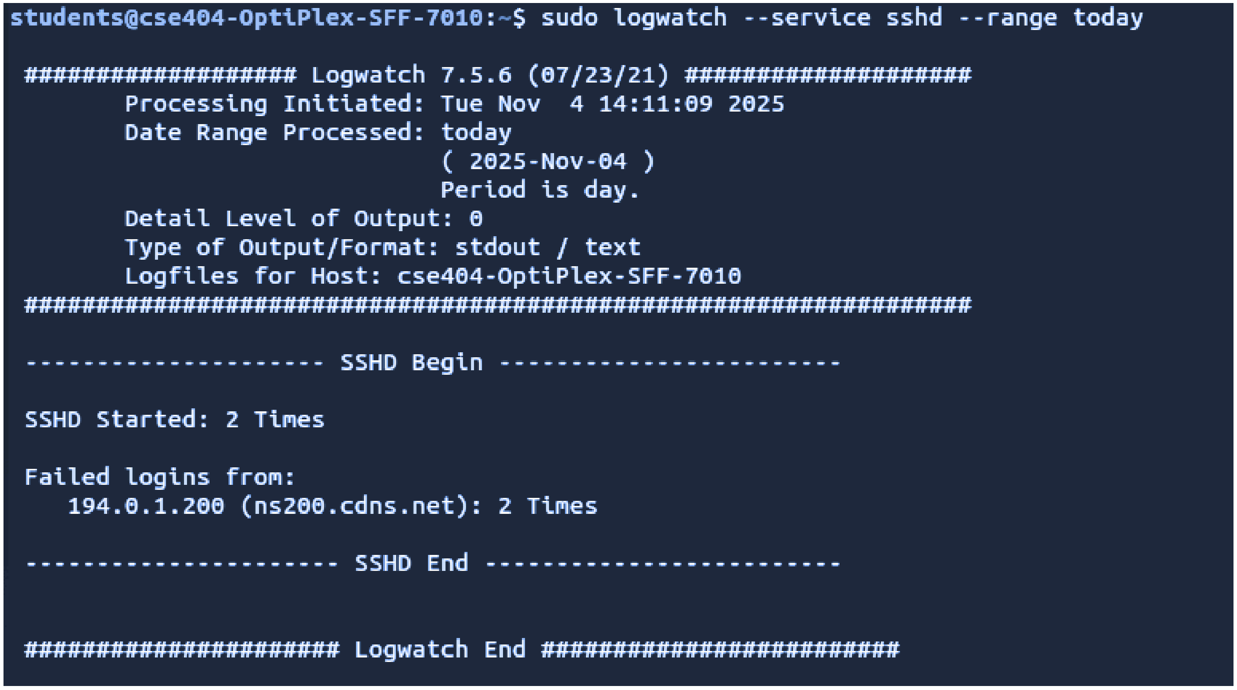
Output: HOST::::



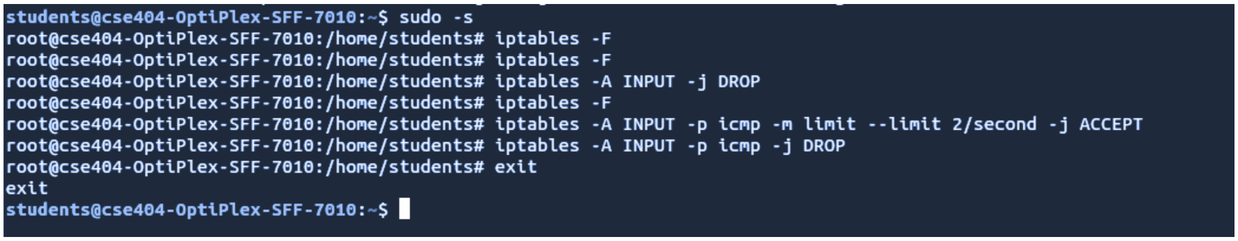
```
students@cse-404-OptiPlex-SFF-7010:~$ sudo snort -c /etc/snort/snort.conf -Q -A console
Enabling inline operation
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
/etc/snort/snort.conf(69) Var 'HOME_NET' redefined.
/etc/snort/snort.conf(72) Var 'EXTERNAL_NET' redefined.
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702
4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:
8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 30
37 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 81
18 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 500
02 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
```



```
===================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        14581 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:        11464 ( 78.623%)
       Frag:          306 (  2.099%)
       ICMP:            0 (  0.000%)
        UDP:         9317 ( 63.898%)
        TCP:         1708 ( 11.714%)
        IP6:         3118 ( 21.384%)
    IP6 Ext:         3296 ( 22.605%)
   IP6 Opts:          178 (  1.221%)
      Frag6:            0 (  0.000%)
      ICMP6:         1032 (  7.078%)
       UDP6:         2085 ( 14.299%)
       TCP6:            0 (  0.000%)
     Teredo:            1 (  0.007%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:          115 (  0.789%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:          115 (  0.789%)
      Other:           69 (  0.473%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:        14581
===================================================
Snort exiting
```

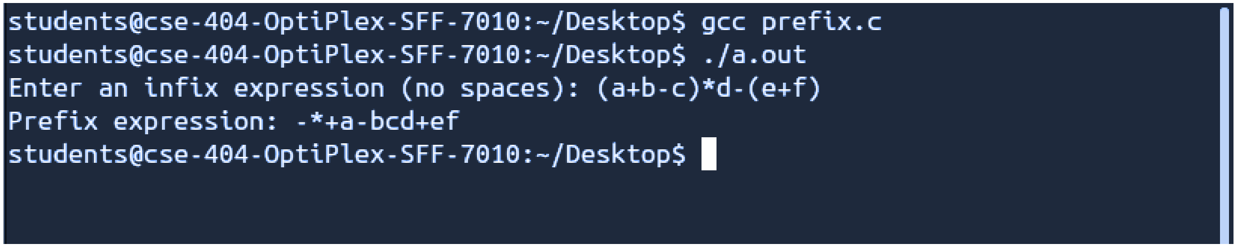


```
students@cse404-OptiPlex-SFF-7010:~$ sudo logwatch --service sshd --range today

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Nov  4 14:11:09 2025
        Date Range Processed: today
                              ( 2025-Nov-04 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: cse404-OptiPlex-SFF-7010
 ##################################################################

 --------------------- SSHD Begin ------------------------

 SSHD Started: 2 Times

 Failed logins from:
    194.0.1.200 (ns200.cdns.net): 2 Times

 ---------------------- SSHD End -------------------------


 ###################### Logwatch End #########################
```

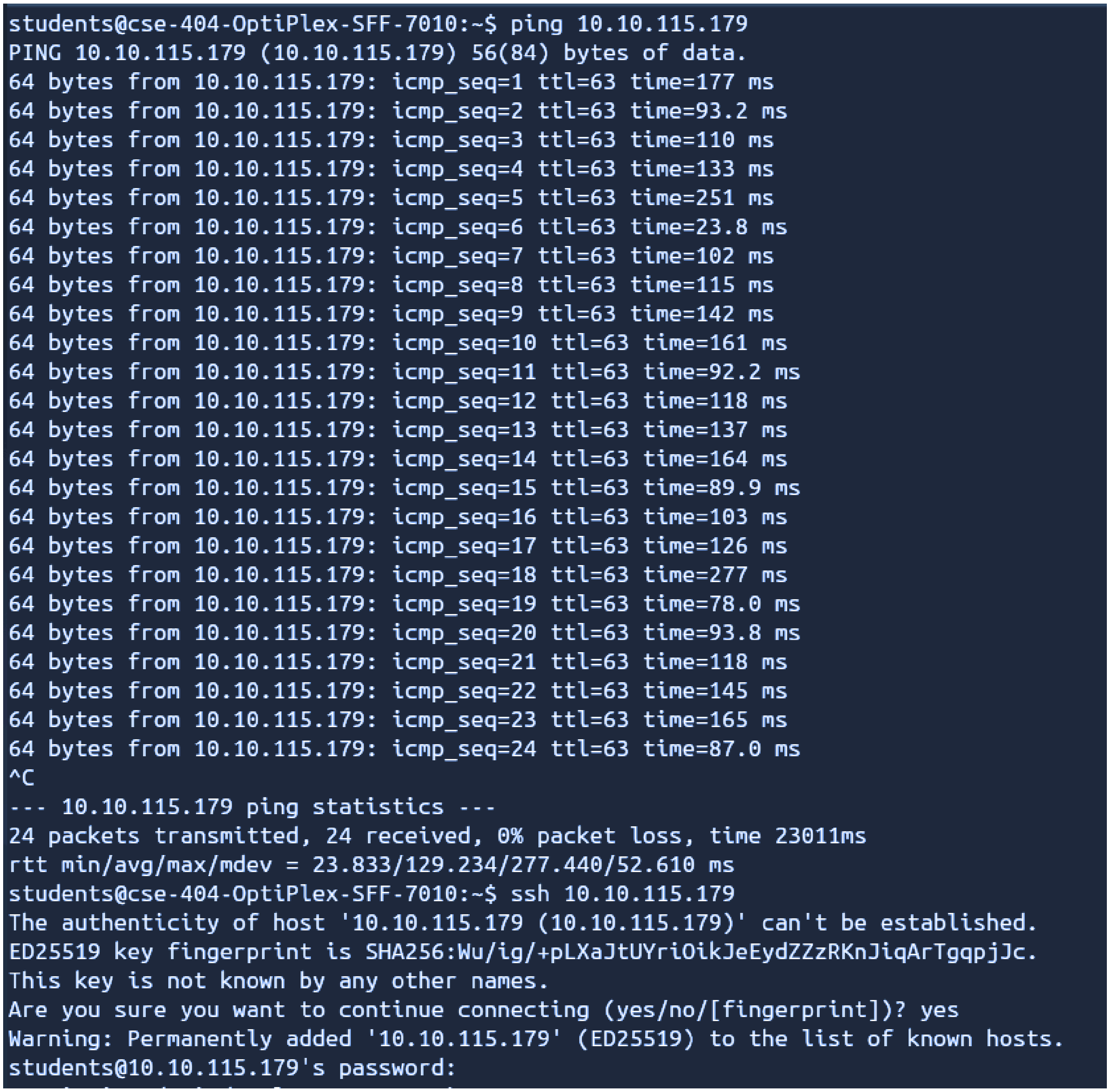


```
students@cse404-OptiPlex-SFF-7010:~$ sudo -s
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -A INPUT -j DROP
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -A INPUT -p icmp -m limit --limit 2/second -j ACCEPT
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -A INPUT -p icmp -j DROP
root@cse404-OptiPlex-SFF-7010:/home/students# exit
exit
students@cse404-OptiPlex-SFF-7010:~$ 
```

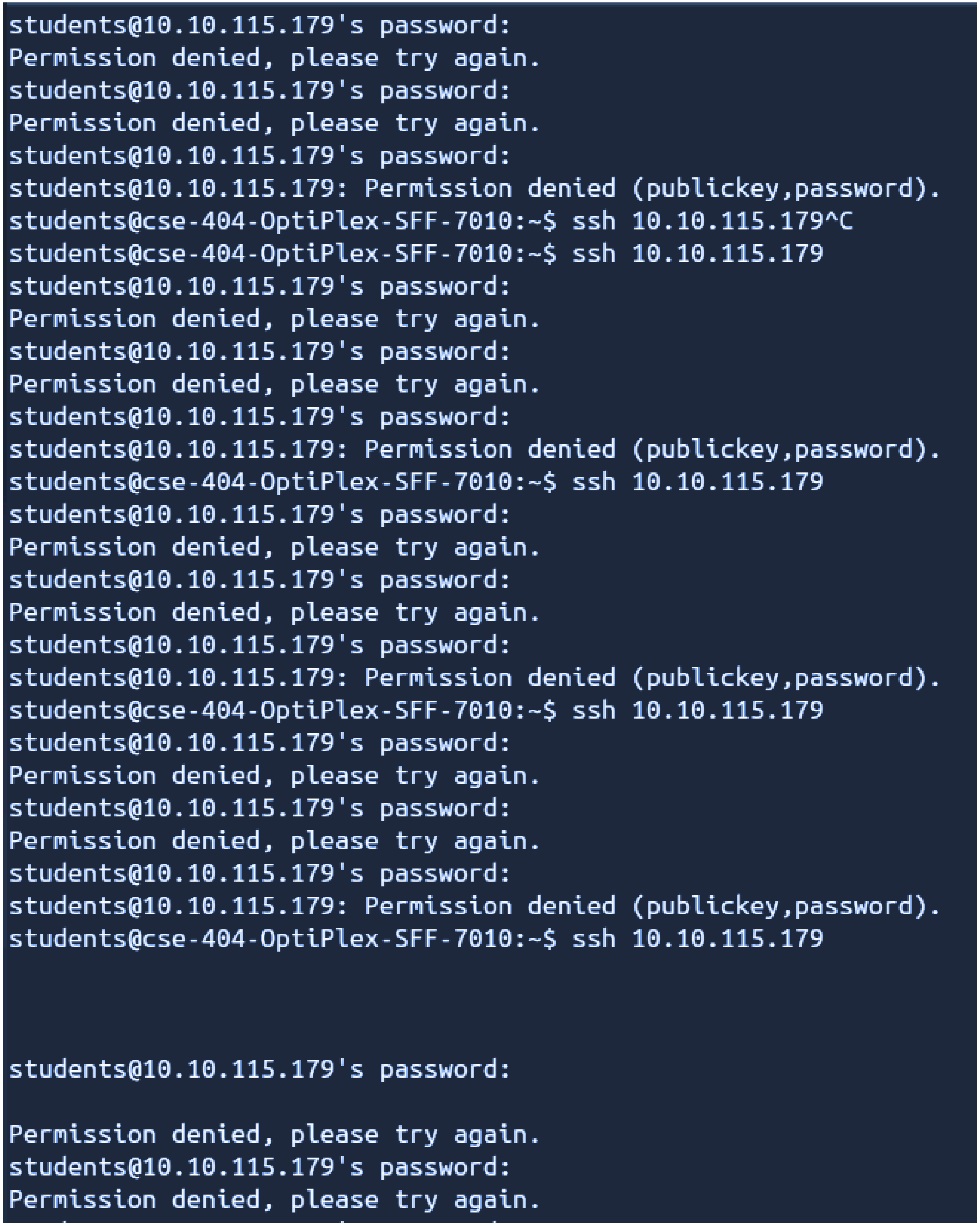
ATTACKER:



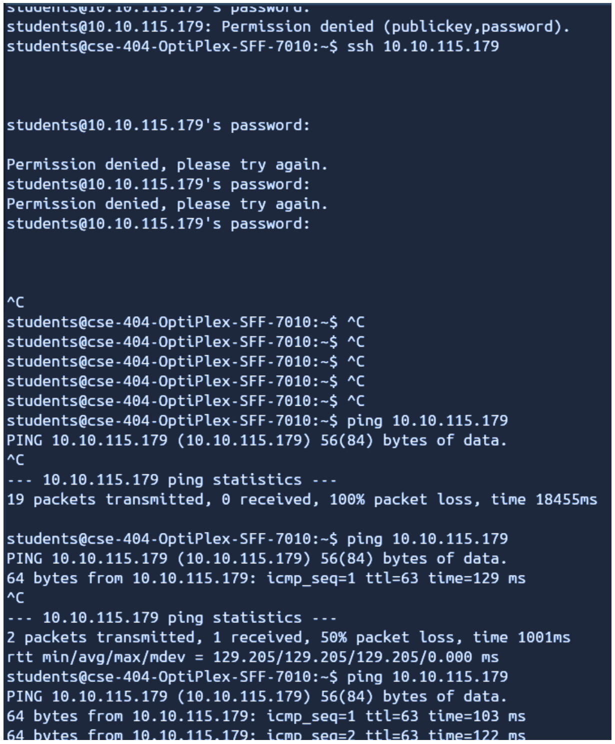
```
students@cse-404-OptiPlex-SFF-7010:~/Desktop$ gcc prefix.c
students@cse-404-OptiPlex-SFF-7010:~/Desktop$ ./a.out
Enter an infix expression (no spaces): (a+b-c)*d-(e+f)
Prefix expression: -*+a-bcd+ef
students@cse-404-OptiPlex-SFF-7010:~/Desktop$ 
```



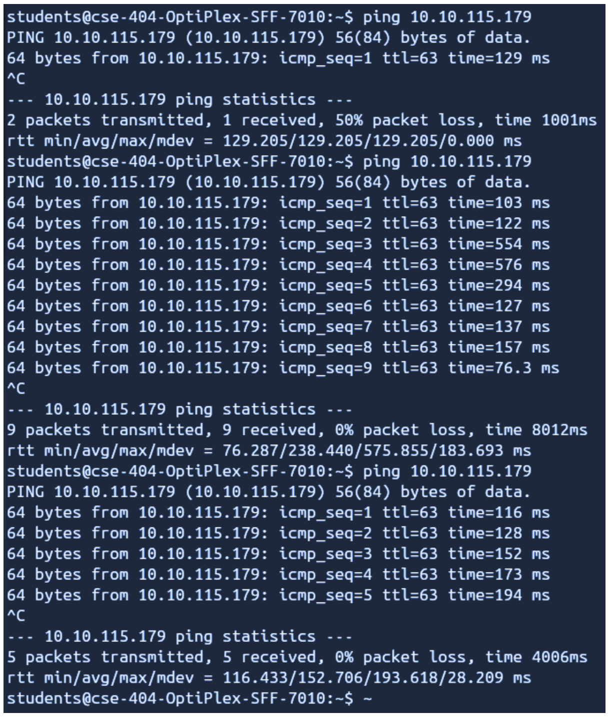
```
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=177 ms
64 bytes from 10.10.115.179: icmp_seq=2 ttl=63 time=93.2 ms
64 bytes from 10.10.115.179: icmp_seq=3 ttl=63 time=110 ms
64 bytes from 10.10.115.179: icmp_seq=4 ttl=63 time=133 ms
64 bytes from 10.10.115.179: icmp_seq=5 ttl=63 time=251 ms
64 bytes from 10.10.115.179: icmp_seq=6 ttl=63 time=23.8 ms
64 bytes from 10.10.115.179: icmp_seq=7 ttl=63 time=102 ms
64 bytes from 10.10.115.179: icmp_seq=8 ttl=63 time=115 ms
64 bytes from 10.10.115.179: icmp_seq=9 ttl=63 time=142 ms
64 bytes from 10.10.115.179: icmp_seq=10 ttl=63 time=161 ms
64 bytes from 10.10.115.179: icmp_seq=11 ttl=63 time=92.2 ms
64 bytes from 10.10.115.179: icmp_seq=12 ttl=63 time=118 ms
64 bytes from 10.10.115.179: icmp_seq=13 ttl=63 time=137 ms
64 bytes from 10.10.115.179: icmp_seq=14 ttl=63 time=164 ms
64 bytes from 10.10.115.179: icmp_seq=15 ttl=63 time=89.9 ms
64 bytes from 10.10.115.179: icmp_seq=16 ttl=63 time=103 ms
64 bytes from 10.10.115.179: icmp_seq=17 ttl=63 time=126 ms
64 bytes from 10.10.115.179: icmp_seq=18 ttl=63 time=277 ms
64 bytes from 10.10.115.179: icmp_seq=19 ttl=63 time=78.0 ms
64 bytes from 10.10.115.179: icmp_seq=20 ttl=63 time=93.8 ms
64 bytes from 10.10.115.179: icmp_seq=21 ttl=63 time=118 ms
64 bytes from 10.10.115.179: icmp_seq=22 ttl=63 time=145 ms
64 bytes from 10.10.115.179: icmp_seq=23 ttl=63 time=165 ms
64 bytes from 10.10.115.179: icmp_seq=24 ttl=63 time=87.0 ms
^C
--- 10.10.115.179 ping statistics ---
24 packets transmitted, 24 received, 0% packet loss, time 23011ms
rtt min/avg/max/mdev = 23.833/129.234/277.440/52.610 ms
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179
The authenticity of host '10.10.115.179 (10.10.115.179)' can't be established.
ED25519 key fingerprint is SHA256:Wu/ig/+pLXaJtUYriOikJeEydZZzRKnJiqArTgqpjJc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.115.179' (ED25519) to the list of known hosts.
students@10.10.115.179's password:
```



```
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
students@10.10.115.179: Permission denied (publickey,password).
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179^C
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
students@10.10.115.179: Permission denied (publickey,password).
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
students@10.10.115.179: Permission denied (publickey,password).
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:
students@10.10.115.179: Permission denied (publickey,password).
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179



students@10.10.115.179's password:

Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
```



```
students@10.10.115.179's password:
students@10.10.115.179: Permission denied (publickey,password).
students@cse-404-OptiPlex-SFF-7010:~$ ssh 10.10.115.179



students@10.10.115.179's password:

Permission denied, please try again.
students@10.10.115.179's password:
Permission denied, please try again.
students@10.10.115.179's password:



^C
students@cse-404-OptiPlex-SFF-7010:~$ ^C
students@cse-404-OptiPlex-SFF-7010:~$ ^C
students@cse-404-OptiPlex-SFF-7010:~$ ^C
students@cse-404-OptiPlex-SFF-7010:~$ ^C
students@cse-404-OptiPlex-SFF-7010:~$ ^C
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
^C
--- 10.10.115.179 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18455ms

students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=129 ms
^C
--- 10.10.115.179 ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 129.205/129.205/129.205/0.000 ms
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=103 ms
64 bytes from 10.10.115.179: icmp_seq=2 ttl=63 time=122 ms
```



```
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=129 ms
^C
--- 10.10.115.179 ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 129.205/129.205/129.205/0.000 ms
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=103 ms
64 bytes from 10.10.115.179: icmp_seq=2 ttl=63 time=122 ms
64 bytes from 10.10.115.179: icmp_seq=3 ttl=63 time=554 ms
64 bytes from 10.10.115.179: icmp_seq=4 ttl=63 time=576 ms
64 bytes from 10.10.115.179: icmp_seq=5 ttl=63 time=294 ms
64 bytes from 10.10.115.179: icmp_seq=6 ttl=63 time=127 ms
64 bytes from 10.10.115.179: icmp_seq=7 ttl=63 time=137 ms
64 bytes from 10.10.115.179: icmp_seq=8 ttl=63 time=157 ms
64 bytes from 10.10.115.179: icmp_seq=9 ttl=63 time=76.3 ms
^C
--- 10.10.115.179 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 76.287/238.440/575.855/183.693 ms
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=116 ms
64 bytes from 10.10.115.179: icmp_seq=2 ttl=63 time=128 ms
64 bytes from 10.10.115.179: icmp_seq=3 ttl=63 time=152 ms
64 bytes from 10.10.115.179: icmp_seq=4 ttl=63 time=173 ms
64 bytes from 10.10.115.179: icmp_seq=5 ttl=63 time=194 ms
^C
--- 10.10.115.179 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 116.433/152.706/193.618/28.209 ms
students@cse-404-OptiPlex-SFF-7010:~$ ~
```

Conclusion : In summary, intrusion detection systems (IDS) are vital for identifying and responding to malicious activities in networks and systems. Network-based (NIDS) and host-based (HIDS) IDS work together to provide comprehensive protection—NIDS monitors network traffic, while HIDS analyzes host activities. Together, they strengthen overall cybersecurity and help prevent potential threats.