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	Pratham Masurkar
Class	TE CSE – 'A'
UID	2023800056
Subject	Cryptography and Network Security

Aim:

i) To implement Network Intrusion Detection System using SNORT:

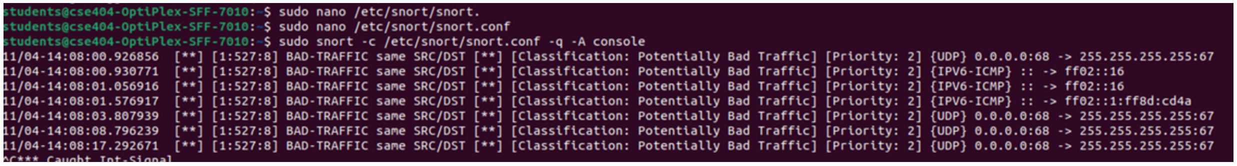
ii)Host based Intrusion Detection System using Logwatch
iii) Event Correlation Analysis (ECA) and iv) Building a Professional Firewall with Linux and Iptables andWindows Firewall

Problem Statement :

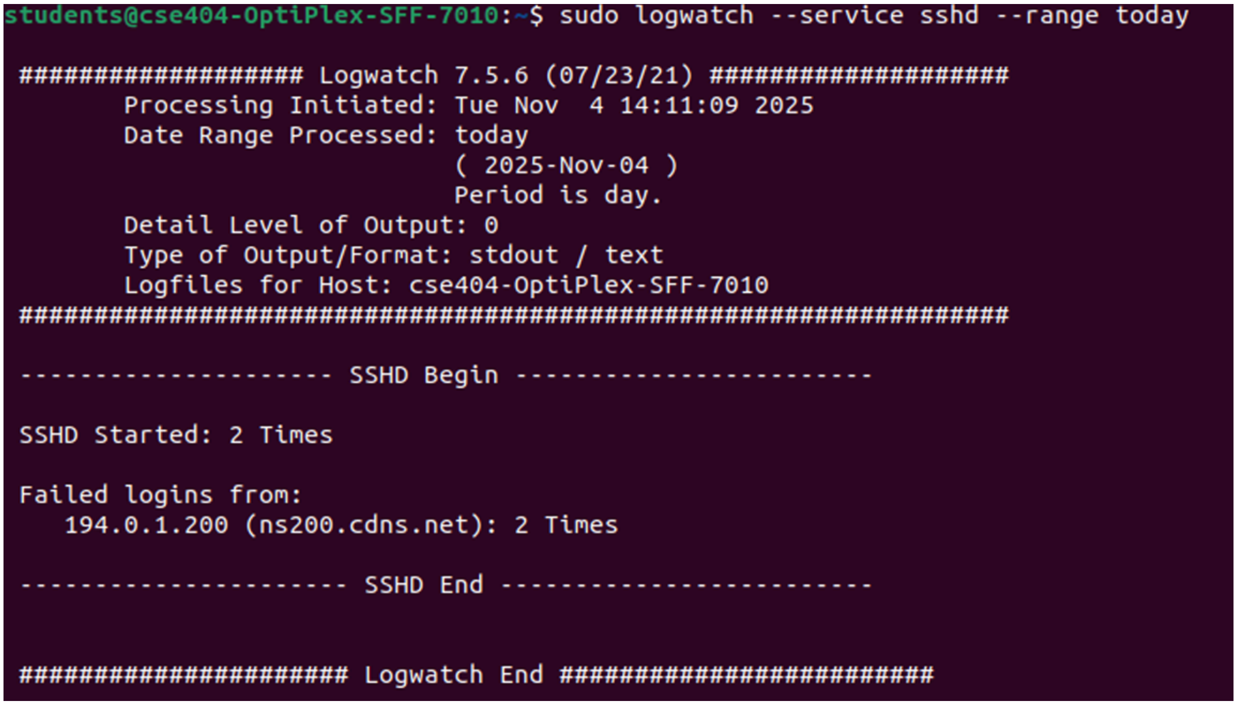
An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.Some systems may attempt to stop an intrusion attempt but this is neither required nor expected 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

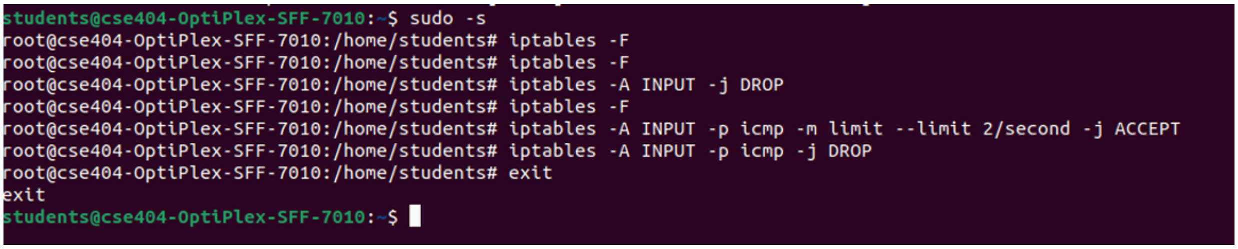
OUTPUT : HOST



```
students@cse404-OptiPlex-SFF-7010:~$ sudo nano /etc/snort/snort.
students@cse404-OptiPlex-SFF-7010:~$ sudo nano /etc/snort/snort.conf
students@cse404-OptiPlex-SFF-7010:~$ sudo snort -c /etc/snort/snort.conf -q -A console
11/04-14:08:00.926856  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
11/04-14:08:00.930771  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
11/04-14:08:01.056916  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
11/04-14:08:01.576917  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ff8d:cd4a
11/04-14:08:03.807939  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
11/04-14:08:08.796239  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
11/04-14:08:17.292671  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
^C*** Caught Int-Signal
```

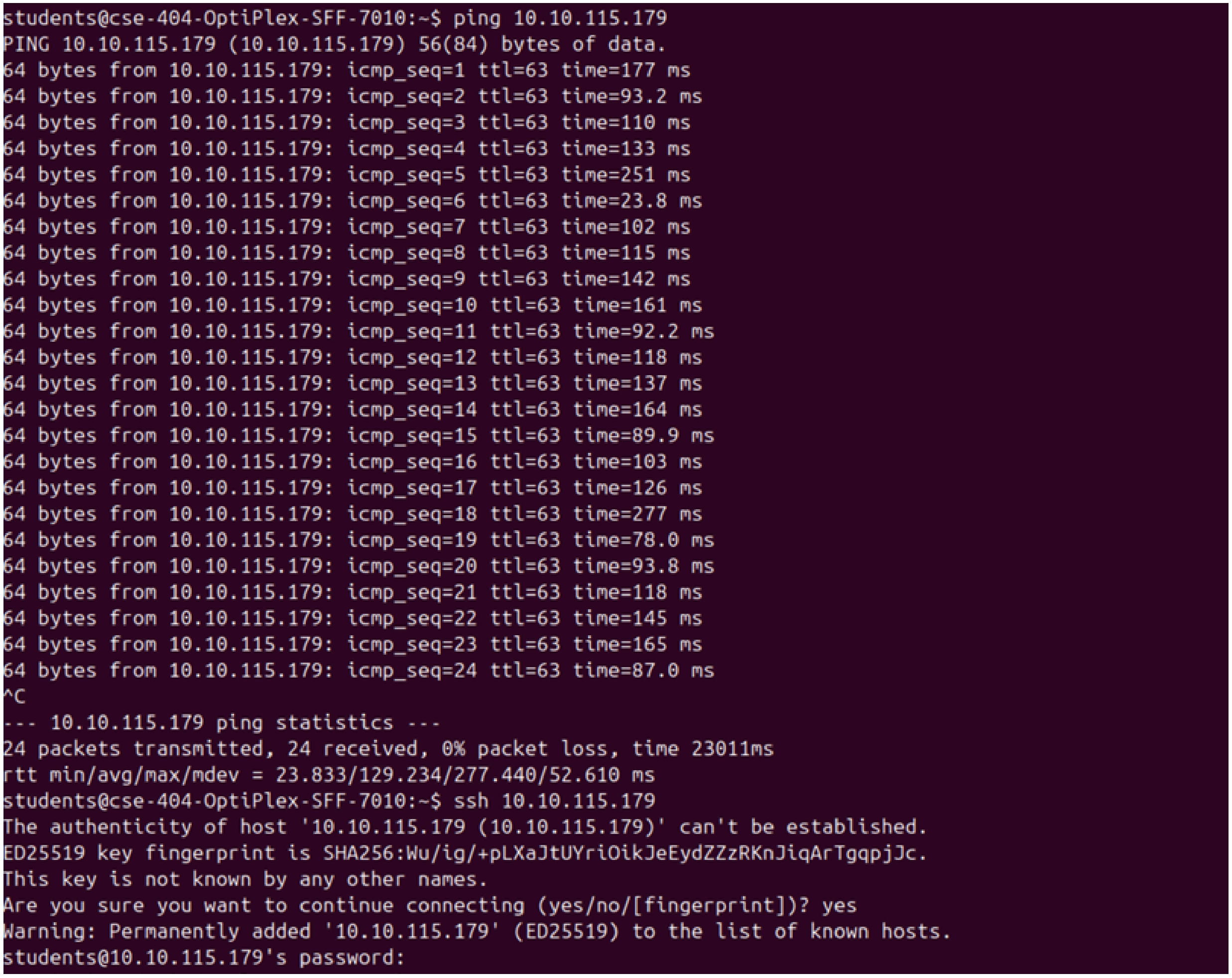


```
students@cse404-OptiPlex-SFF-7010:~$ sudo logwatch --service sshd --range today

 ################### 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 #########################
```

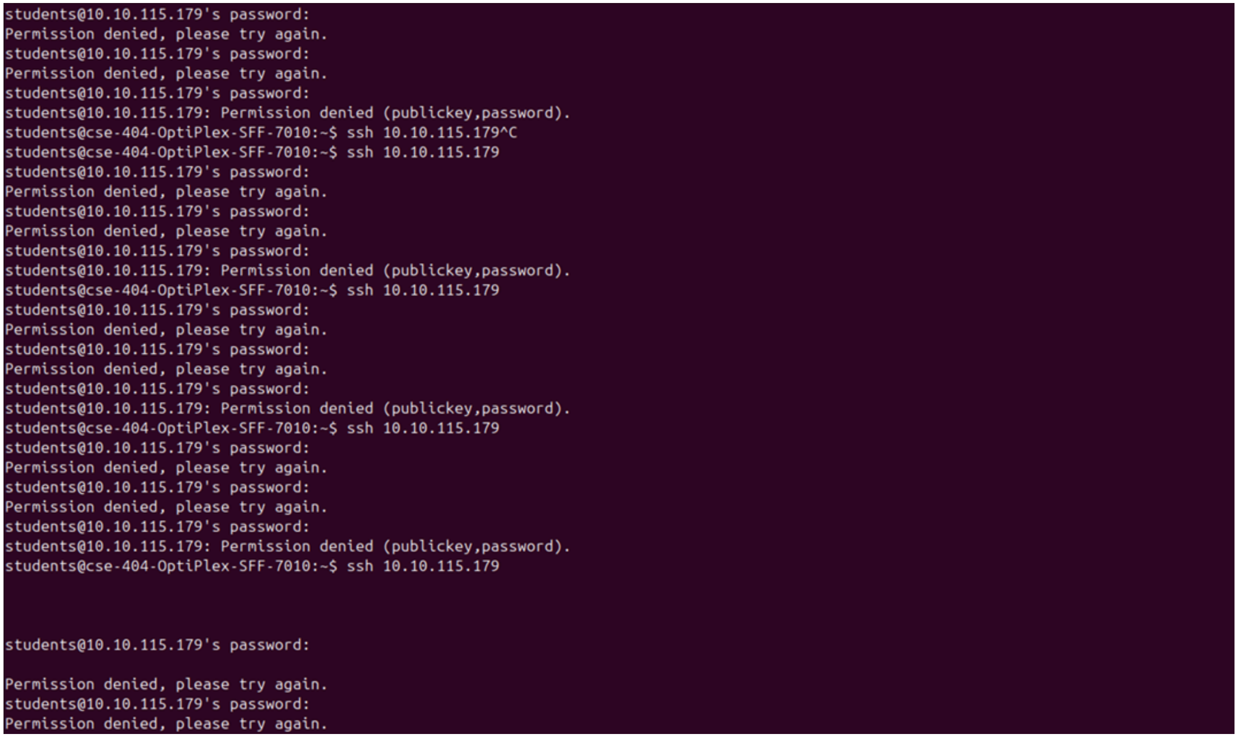


```
students@cse404-OptiPlex-SFF-7010:~$ sudo -s
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -A INPUT -j DROP
root@cse404-OptiPlex-SFF-7010:/home/students# iptables -F
root@cse404-OptiPlex-SFF-7010:/home/students# 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:~$ █
```

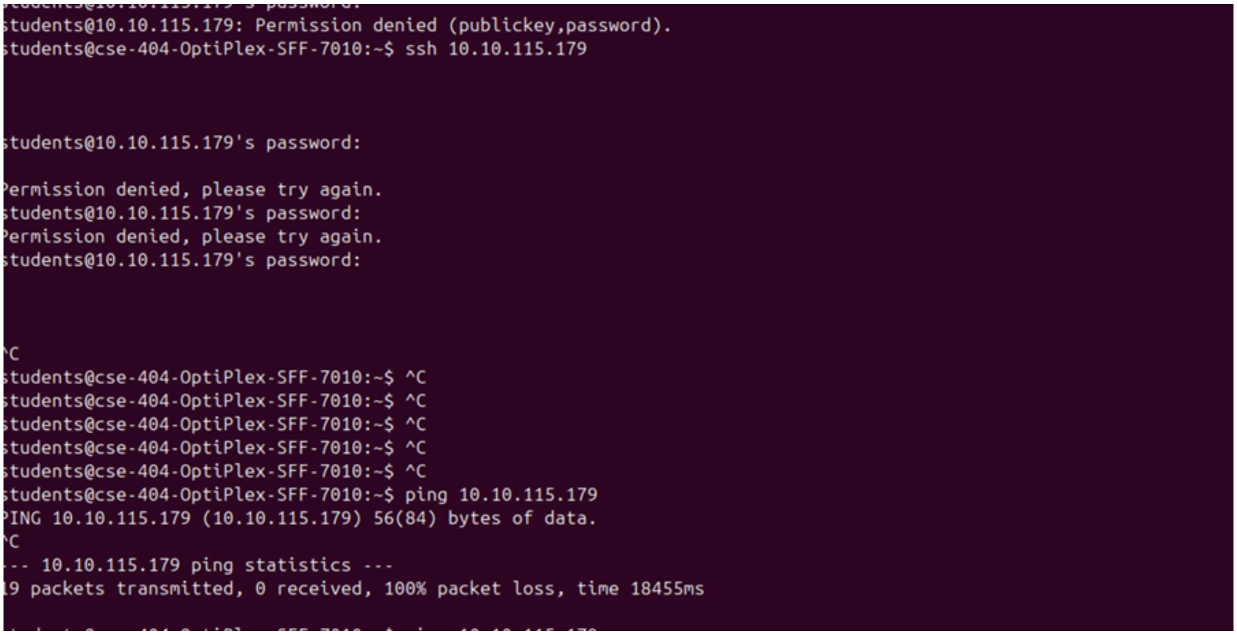
ATTACKER :



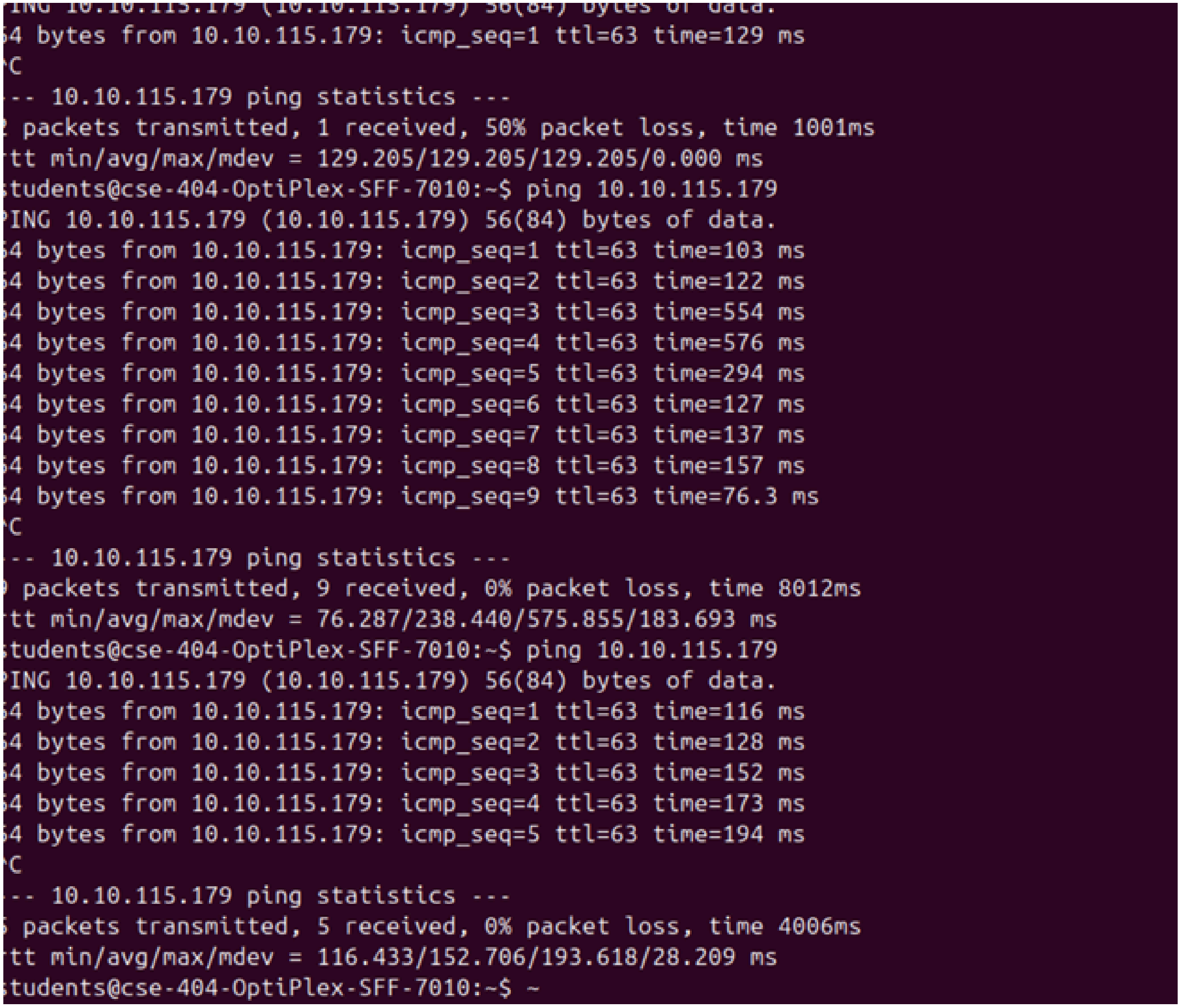
```
students@cse-404-OptiPlex-SFF-7010:~$ ping 10.10.115.179
PING 10.10.115.179 (10.10.115.179) 56(84) bytes of data.
64 bytes from 10.10.115.179: icmp_seq=1 ttl=63 time=177 ms
64 bytes from 10.10.115.179: icmp_seq=2 ttl=63 time=93.2 ms
64 bytes from 10.10.115.179: icmp_seq=3 ttl=63 time=110 ms
64 bytes 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
```



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

Conclusion:

Intrusion Detection Systems (IDS) play a crucial role in detecting and responding to malicious behavior within networks and devices. Network-based IDS (NIDS) monitors traffic across the network, while host-based IDS (HIDS) examines activities occurring on individual systems. When used together, they provide layered security, enhance overall protection, and help prevent potential cyber threats.