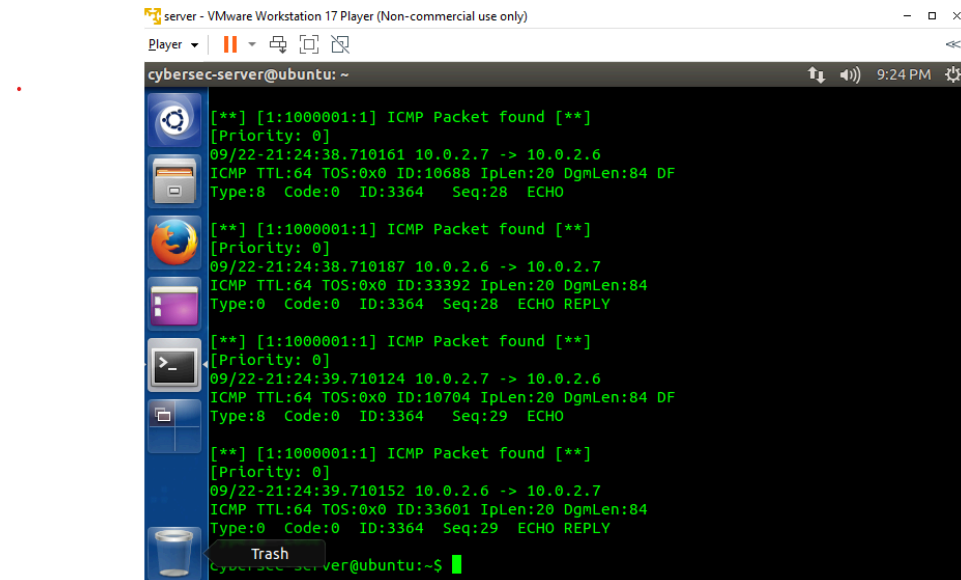


Task 1

Have you received alerts from the ping attempt?

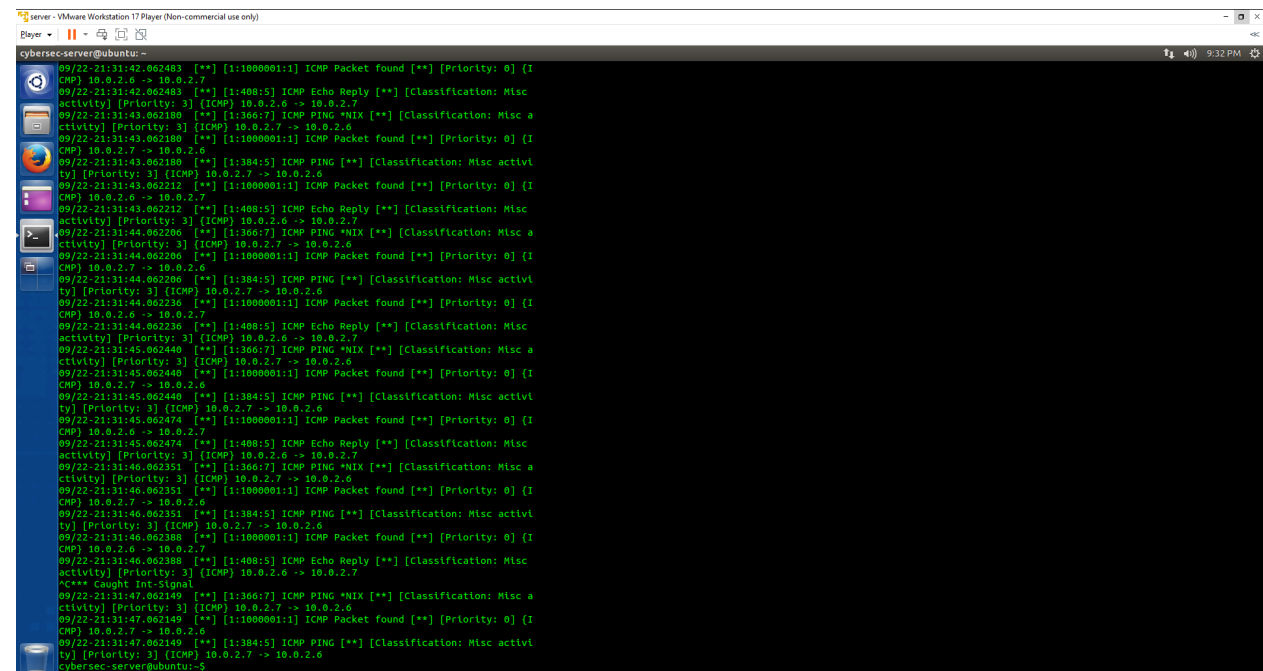
Yes i have. Screenshot below



Task 2

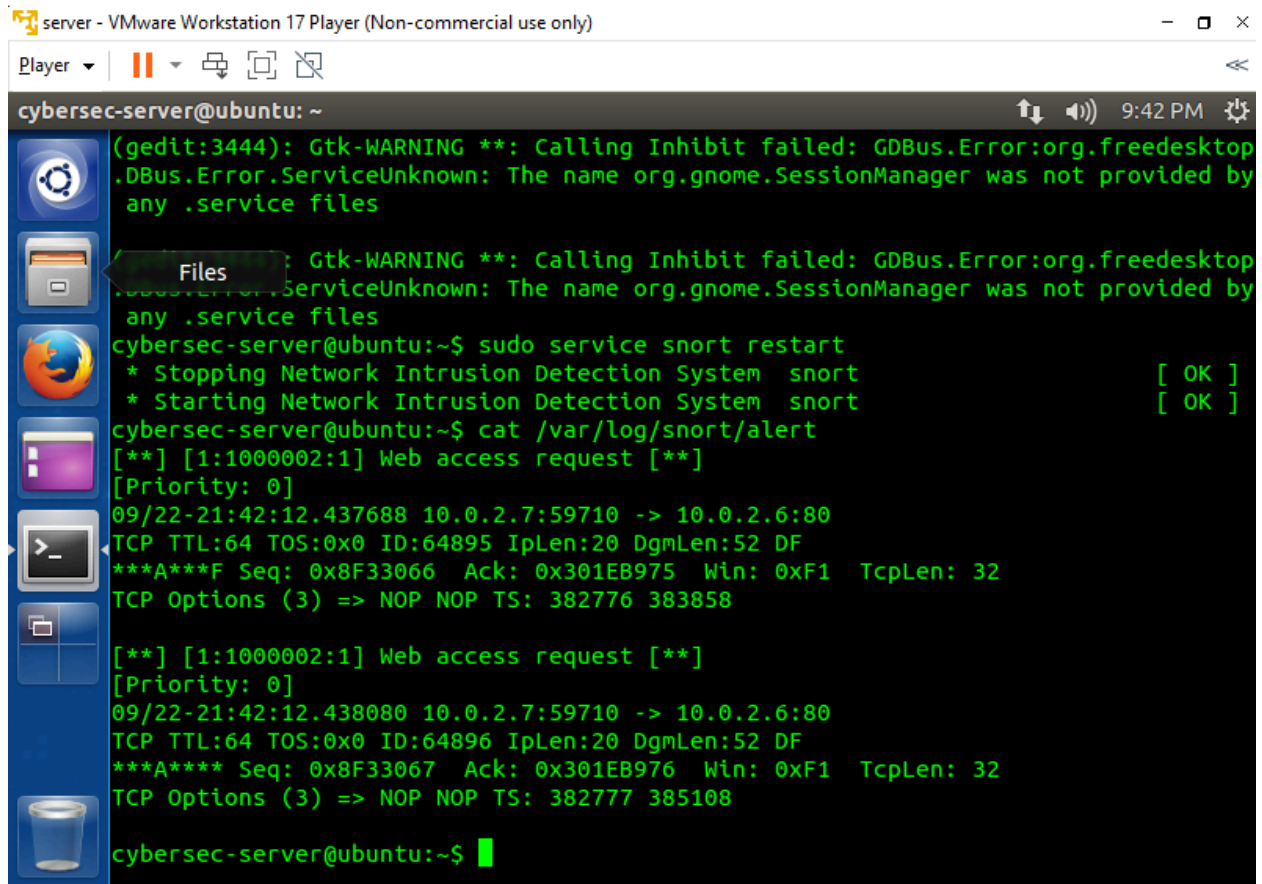
Have you received alert messages for the ICMP packets in IDS mode?

Yes.



Task 3

Q3. Have you received alert messages for Web access? Please provide screenshot



```
server - VMware Workstation 17 Player (Non-commercial use only)
Player
cybersec-server@ubuntu: ~
(gedit:3444): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
Files
cybersec-server@ubuntu:~$ sudo service snort restart
* Stopping Network Intrusion Detection System snort [ OK ]
* Starting Network Intrusion Detection System snort [ OK ]
cybersec-server@ubuntu:~$ cat /var/log/snort/alert
[**] [1:1000002:1] Web access request [**]
[Priority: 0]
09/22-21:42:12.437688 10.0.2.7:59710 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:64895 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x8F33066 Ack: 0x301EB975 Win: 0xF1 TcpLen: 32
TCP Options (3) => NOP NOP TS: 382776 383858

[**] [1:1000002:1] Web access request [**]
[Priority: 0]
09/22-21:42:12.438080 10.0.2.7:59710 -> 10.0.2.6:80
TCP TTL:64 TOS:0x0 ID:64896 IpLen:20 DgmLen:52 DF
***A*** Seq: 0x8F33067 Ack: 0x301EB976 Win: 0xF1 TcpLen: 32
TCP Options (3) => NOP NOP TS: 382777 385108

cybersec-server@ubuntu:~$
```

Q4. Have you received alert messages for Source Quench packets? Please provide screenshot to support your answer

```
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/22-21:49:36.841898 10.0.2.6 -> 10.0.2.8
ICMP TTL:255 TOS:0x0 ID:12880 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.8 -> 10.0.2.6
ICMP TTL:64 TOS:0x0 ID:8006 IpLen:20 DgmLen:84 DF
Type: 8 Code: 0 Csum: 7133 Id: 2886 SeqNo: 12
** END OF DUMP

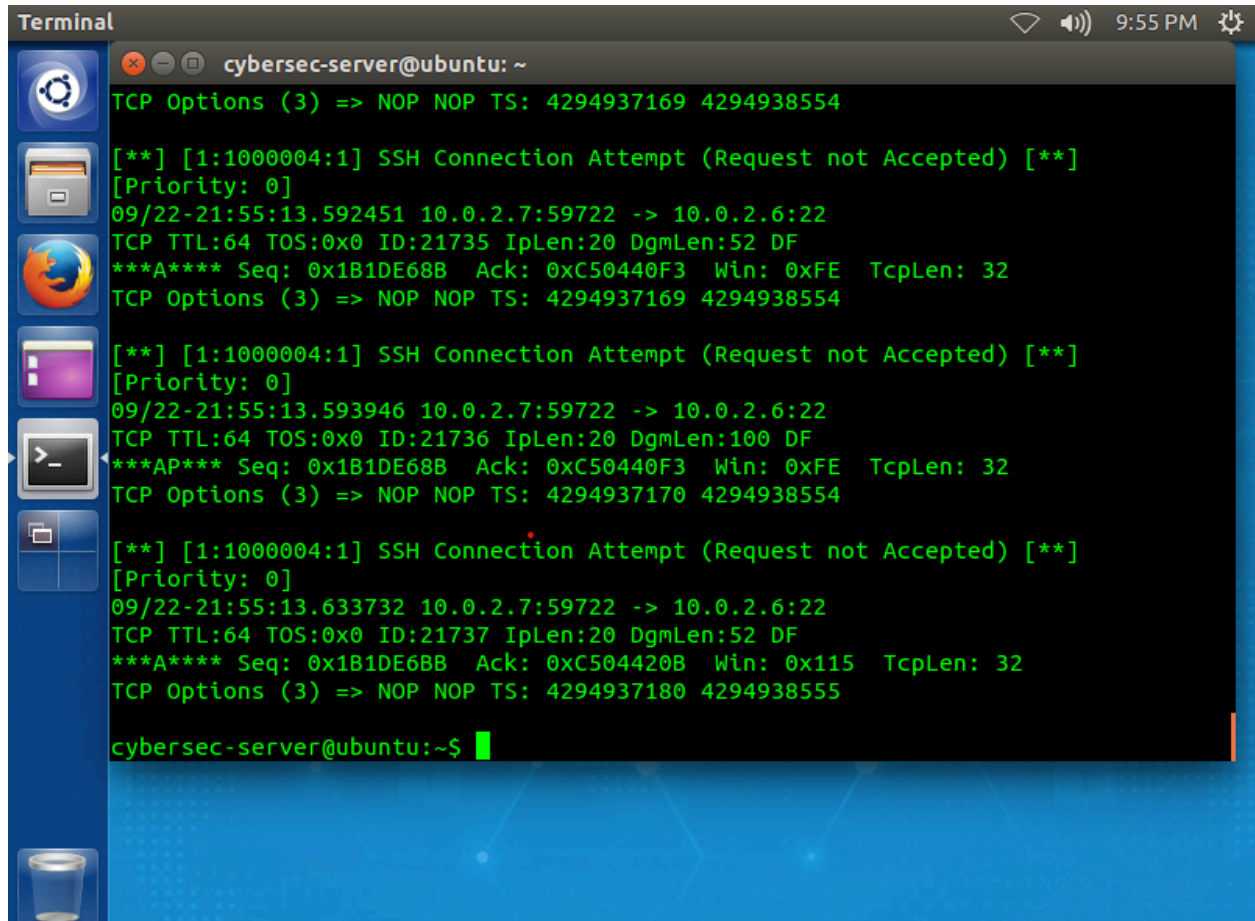
[**] [1:1000003:1] ICMP source quench [**]
[Priority: 0]
09/22-21:49:36.841903 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:5112 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:7886 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 9181 Id: 2886 SeqNo: 12
** END OF DUMP

[**] [1:1000001:1] ICMP Packet found [**]
[Priority: 0]
09/22-21:49:36.841903 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:5112 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:7886 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 9181 Id: 2886 SeqNo: 12
** END OF DUMP

[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/22-21:49:36.841903 10.0.2.6 -> 10.0.2.6
ICMP TTL:255 TOS:0x0 ID:5112 IpLen:20 DgmLen:56
Type:4 Code:0 SOURCE QUENCH
** ORIGINAL DATAGRAM DUMP:
10.0.2.6 -> 10.0.2.8
ICMP TTL:64 TOS:0x0 ID:7886 IpLen:20 DgmLen:84
Type: 0 Code: 0 Csum: 9181 Id: 2886 SeqNo: 12
```

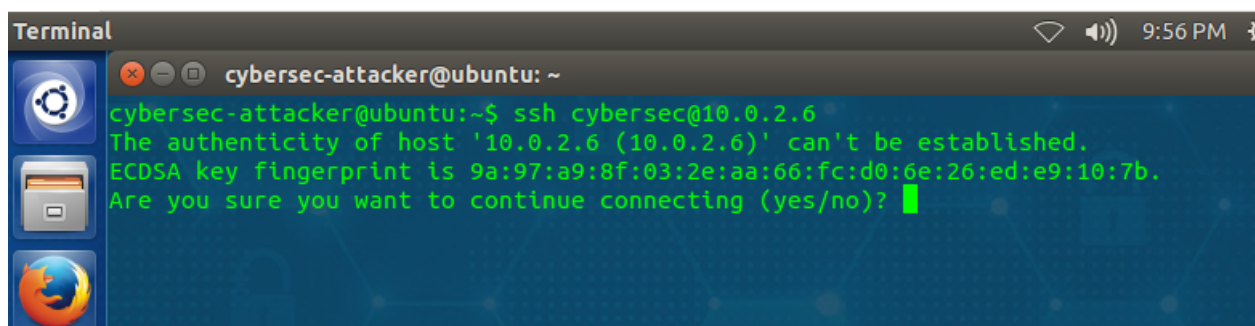
Q5. Have you received alert messages for SSH connection Attempt? Did the connection attempt succeed?

The attempt did not succeed.



The terminal window is titled 'Terminal' and shows the command prompt 'cybersec-server@ubuntu: ~'. The output displays three identical SSH connection attempts from the server to the target IP 10.0.2.6. Each attempt is marked with a green asterisk and the message '[**] [1:1000004:1] SSH Connection Attempt (Request not Accepted) [**]'. The output also shows the priority, timestamp, source and destination IP addresses, TCP TTL, TOS, ID, IP length, DGM length, DF flag, sequence number, acknowledgment number, window size, TCP length, and TCP options (NOP, NOP, TS: 4294937169 4294938554).

```
Terminal
cybersec-server@ubuntu: ~
TCP Options (3) => NOP NOP TS: 4294937169 4294938554
[**] [1:1000004:1] SSH Connection Attempt (Request not Accepted) [**]
[Priority: 0]
09/22-21:55:13.592451 10.0.2.7:59722 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:21735 IpLen:20 DgmLen:52 DF
***A*** Seq: 0x1B1DE68B Ack: 0xC50440F3 Win: 0xFE TcpLen: 32
TCP Options (3) => NOP NOP TS: 4294937169 4294938554
[**] [1:1000004:1] SSH Connection Attempt (Request not Accepted) [**]
[Priority: 0]
09/22-21:55:13.593946 10.0.2.7:59722 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:21736 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0x1B1DE68B Ack: 0xC50440F3 Win: 0xFE TcpLen: 32
TCP Options (3) => NOP NOP TS: 4294937170 4294938554
[**] [1:1000004:1] SSH Connection Attempt (Request not Accepted) [**]
[Priority: 0]
09/22-21:55:13.633732 10.0.2.7:59722 -> 10.0.2.6:22
TCP TTL:64 TOS:0x0 ID:21737 IpLen:20 DgmLen:52 DF
***A*** Seq: 0x1B1DE6BB Ack: 0xC504420B Win: 0x115 TcpLen: 32
TCP Options (3) => NOP NOP TS: 4294937180 4294938555
cybersec-server@ubuntu:~$
```



The terminal window is titled 'Terminal' and shows the command prompt 'cybersec-attacker@ubuntu: ~'. The output displays the command 'ssh cybersec@10.0.2.6' and the resulting error message: 'The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established. ECDSA key fingerprint is 9a:97:a9:8f:03:2e:aa:66:fc:d0:6e:26:ed:e9:10:7b. Are you sure you want to continue connecting (yes/no)?'. The output is in green text.

```
Terminal
cybersec-attacker@ubuntu: ~
cybersec-attacker@ubuntu:~$ ssh cybersec@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is 9a:97:a9:8f:03:2e:aa:66:fc:d0:6e:26:ed:e9:10:7b.
Are you sure you want to continue connecting (yes/no)?
```

Q6. Have you received alert messages for Telnet connection established from Attacker to Server? Did the telnet connection attempt from Attacker to Server succeed? Please provide screenshot to support your answer. Also, mention the rule that was added to "local.rules" to create this alert.

The rule applied is a slightly modified from the previous activity.

```
reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Attack"; sid:1000005;rev:1;)
```

Reject -> Rejects any attempt

TCP -> As Hint suggested, The attack goes through the TCP

10.0.2.6 -> Server IP (Targeted system)

23 -> The attack targets port 23

Msg -> Modified to identify the type of attack

(Screenshots Below)

Player ▾



local.rules (/etc/snort/rules) - gedit



10:04 PM



File Edit View Search Tools Documents Help



Open ▾



Save



Undo



Undo



local.rules x



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any -> any any (msg:"ICMP Packet found";sid:1000001;rev:1;)

alert tcp any any -> 10.0.2.6 80 (msg:"Web access request"; sid:1000002;rev:1;)

alert icmp any any -> any any (msg:"ICMP source
quench";ittype:4;icode:0;sid:1000003;rev:1;)

reject tcp any any -> 10.0.2.6 22 (msg:"SSH Connection Attempt (Request not
Accepted)";sid:1000004;rev:1;)

reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Attack"; sid:1000005;rev:1;)
```

Plain Text ▾

Tab Width: 8 ▾

Ln 1, Col 1

INS

