

IP TABLES - THE LINUX FIREWALL

LAB

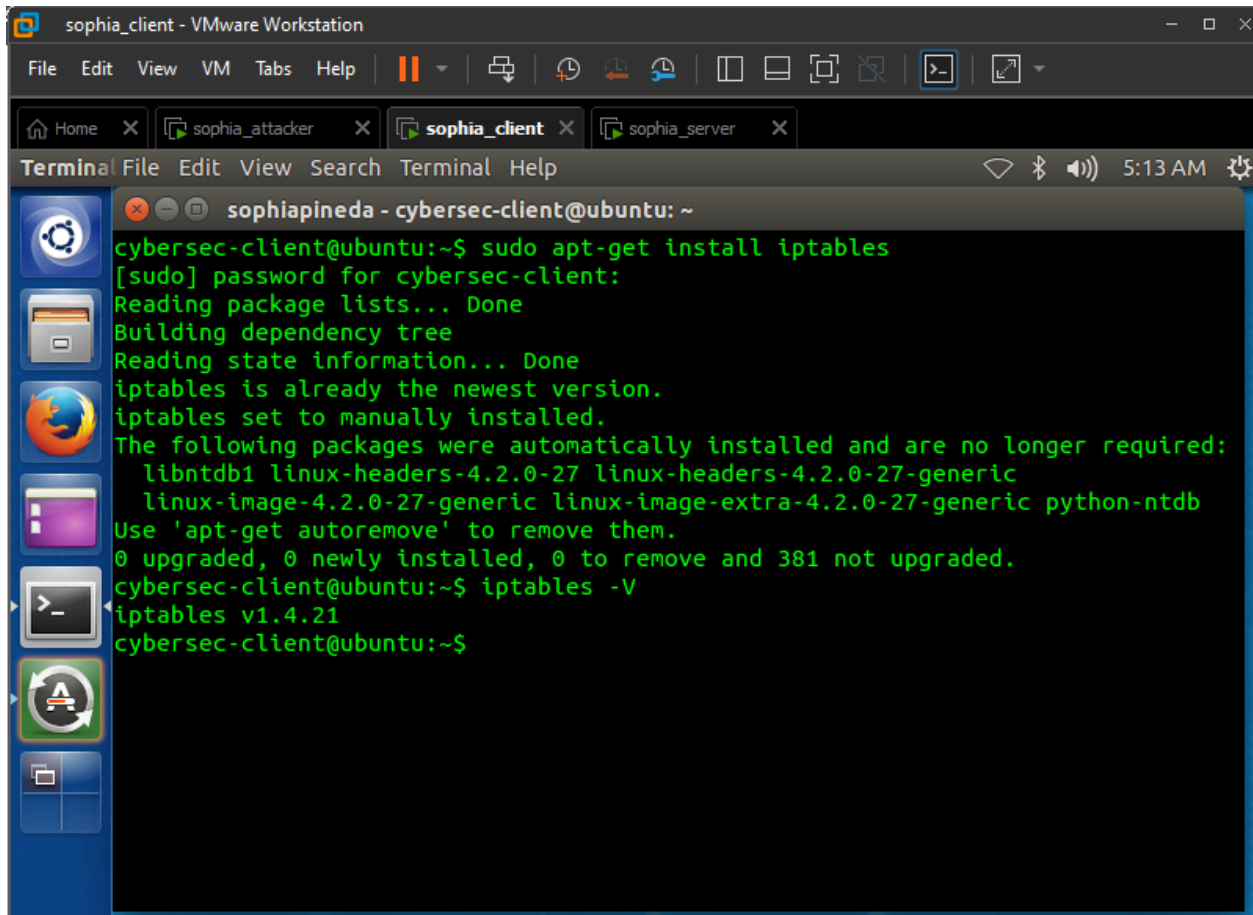
- All three VMS

TASK: CONFIGURE IPTABLES FIREWALL RULES ON CYBER-CLIENT

STEPS

1. Enter `sudo apt-get install iptables` in client VM (install iptables package)
2. Enter `iptables -V` in client VM (Check version of iptables installed in system)

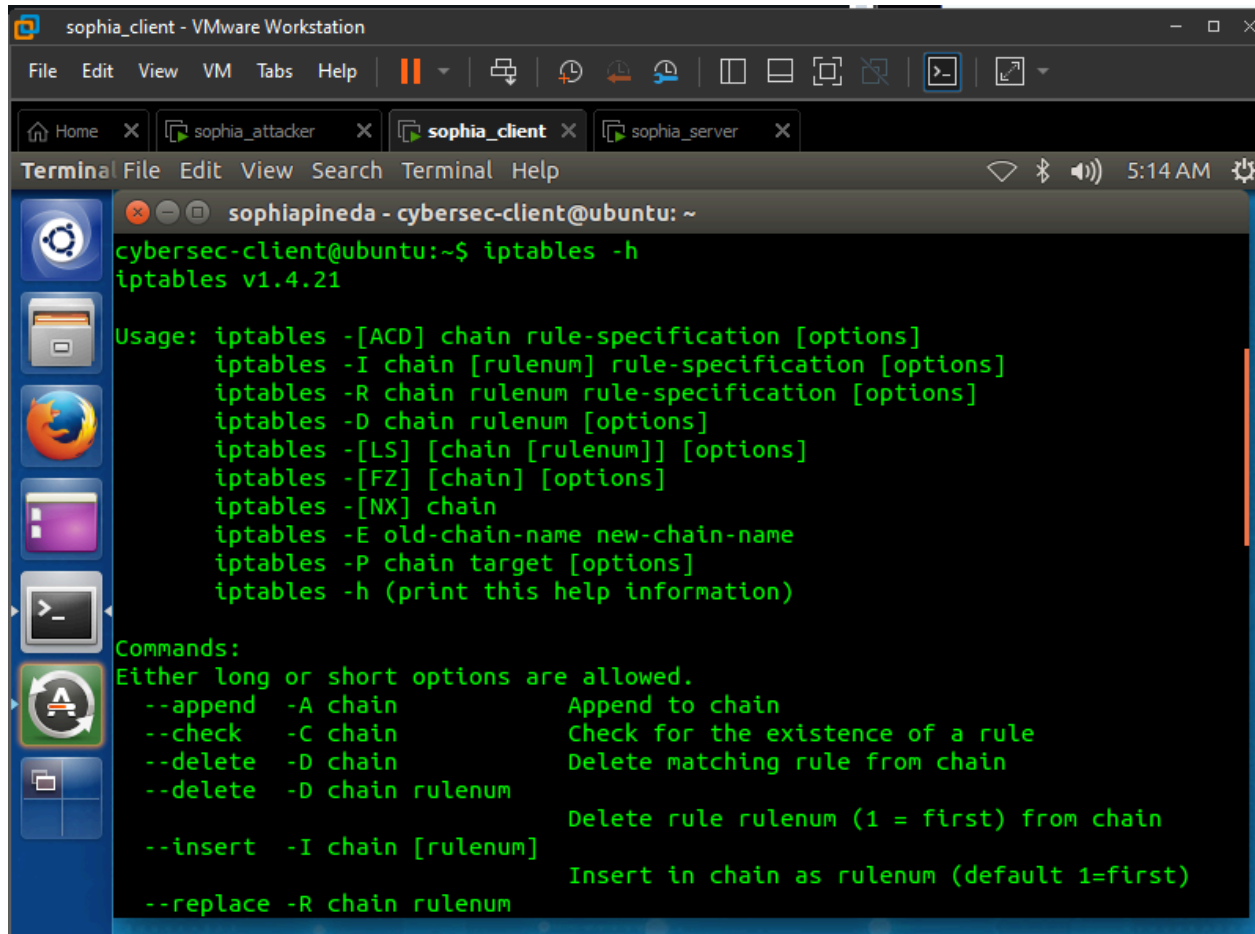
SCREENSHOT



The screenshot shows a VMware Workstation window titled 'sophia_client - VMware Workstation'. It contains three tabs: 'sophia_attacker', 'sophia_client' (active), and 'sophia_server'. The 'sophia_client' tab displays a terminal window with the following output:

```
sophiapineda - cybersec-client@ubuntu: ~  
cybersec-client@ubuntu:~$ sudo apt-get install iptables  
[sudo] password for cybersec-client:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
iptables is already the newest version.  
iptables set to manually installed.  
The following packages were automatically installed and are no longer required:  
  libntdb1 linux-headers-4.2.0-27 linux-headers-4.2.0-27-generic  
  linux-image-4.2.0-27-generic linux-image-extra-4.2.0-27-generic python-ntdb  
Use 'apt-get autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 381 not upgraded.  
cybersec-client@ubuntu:~$ iptables -V  
iptables v1.4.21  
cybersec-client@ubuntu:~$
```

3. Enter `iptables -h` (checks usage of iptables) **SCREENSHOT**



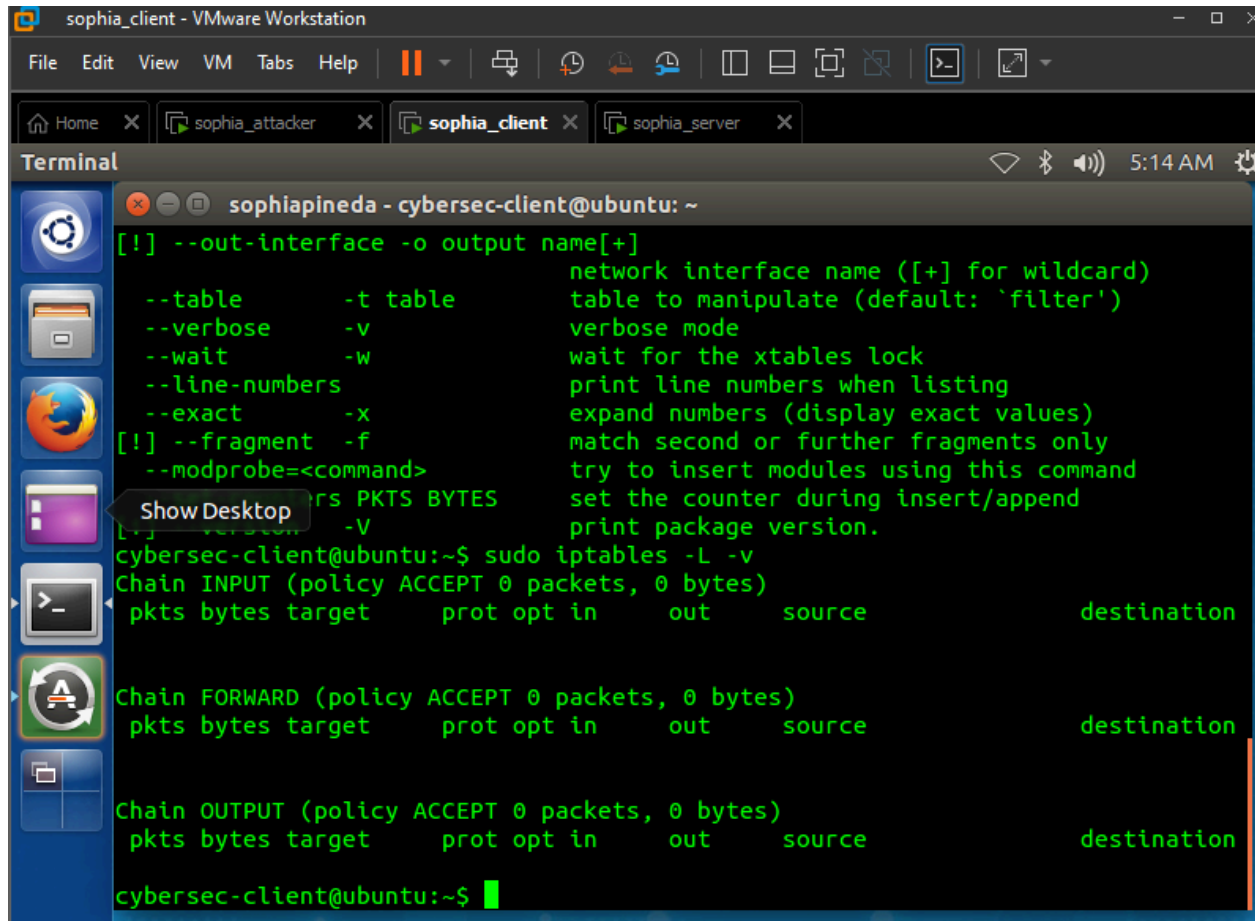
The screenshot shows a VMware Workstation window titled 'sophia_client - VMware Workstation'. It contains four virtual machines: 'sophia_attacker', 'sophia_client', 'sophia_server', and 'sophia_server'. The 'sophia_client' VM is selected, and its terminal window is open. The terminal shows the command 'cybersec-client@ubuntu:~\$ iptables -h' and its output. The output includes the version 'iptables v1.4.21', a usage section, and a list of commands with their descriptions.

```
sophiapineda - cybersec-client@ubuntu: ~
cybersec-client@ubuntu:~$ iptables -h
iptables v1.4.21

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
       iptables -[NX] chain
       iptables -E old-chain-name new-chain-name
       iptables -P chain target [options]
       iptables -h (print this help information)

Commands:
Either long or short options are allowed.
--append -A chain          Append to chain
--check  -C chain          Check for the existence of a rule
--delete -D chain          Delete matching rule from chain
--delete -D chain rulenum  Delete rule rulenum (1 = first) from chain
--insert -I chain [rulenum] Insert in chain as rulenum (default 1=first)
--replace -R chain rulenum
```

4. Enter `sudo iptables -L -v` (checks current iptables chains and checks number of packets accepted or denied) **SCREENSHOT**



```
sophiapineda - cybersec-client@ubuntu: ~  
[!] --out-interface -o output name[+]  
network interface name ([+] for wildcard)  
--table -t table table to manipulate (default: 'filter')  
--verbose -v verbose mode  
--wait -w wait for the xtables lock  
--line-numbers print line numbers when listing  
--exact -x expand numbers (display exact values)  
[!] --fragment -f match second or further fragments only  
--modprobe=<command> try to insert modules using this command  
--counters PKTS BYTES set the counter during insert/append  
[!] --version -V print package version.  
cybersec-client@ubuntu:~$ sudo iptables -L -v  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
cybersec-client@ubuntu:~$
```

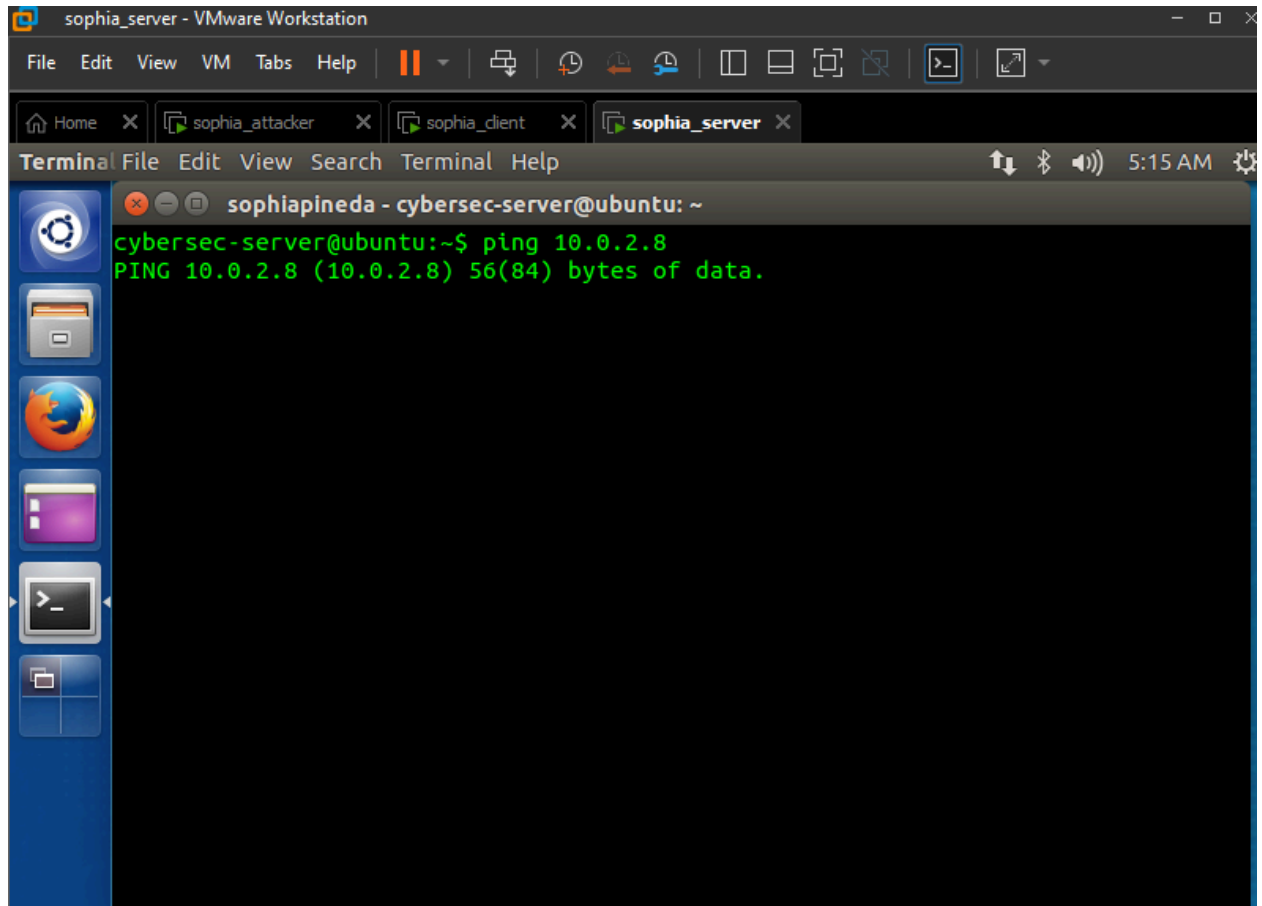
(changes behaviour of chain to drop all traffic) **SCREENSHOT**

5. Enter `sudo iptables -policy INPUT DROP` in client VM
6. Enter `sudo iptables -policy OUTPUT DROP`
7. Enter `sudo iptables -policy FORWARD DROP`

The screenshot shows a VMware Workstation window titled 'sophia_client - VMware Workstation'. It contains three virtual machines: 'sophia_attacker', 'sophia_client', and 'sophia_server'. The 'sophia_client' VM is active, and its terminal window is open. The terminal shows the user 'sophiapineda' at the 'cybersec-client@ubuntu: ~' prompt. The user has entered several commands to configure iptables. The output shows the current state of the iptables chains: FORWARD, OUTPUT, INPUT, and FORWARD, all with a policy of DROP. The user has also entered the command 'sudo iptables -L' to list the rules.

```
sophiapineda - cybersec-client@ubuntu: ~  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in      out     source    destination  
  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in      out     source    destination  
  
cybersec-client@ubuntu:~$ sudo iptables -policy INPUT DROP  
iptables v1.4.21: unknown protocol "olicy" specified  
Try `iptables -h' or 'iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables --policy INPUT DROP  
cybersec-client@ubuntu:~$ sudo iptables --policy OUTPUT DROP  
cybersec-client@ubuntu:~$ sudo iptables --policy FORWARD DROP  
cybersec-client@ubuntu:~$ sudo iptables -L  
Chain INPUT (policy DROP)  
target     prot opt source                destination  
  
Chain FORWARD (policy DROP)  
target     prot opt source                destination  
  
Chain OUTPUT (policy DROP)  
target     prot opt source                destination  
cybersec-client@ubuntu:~$
```

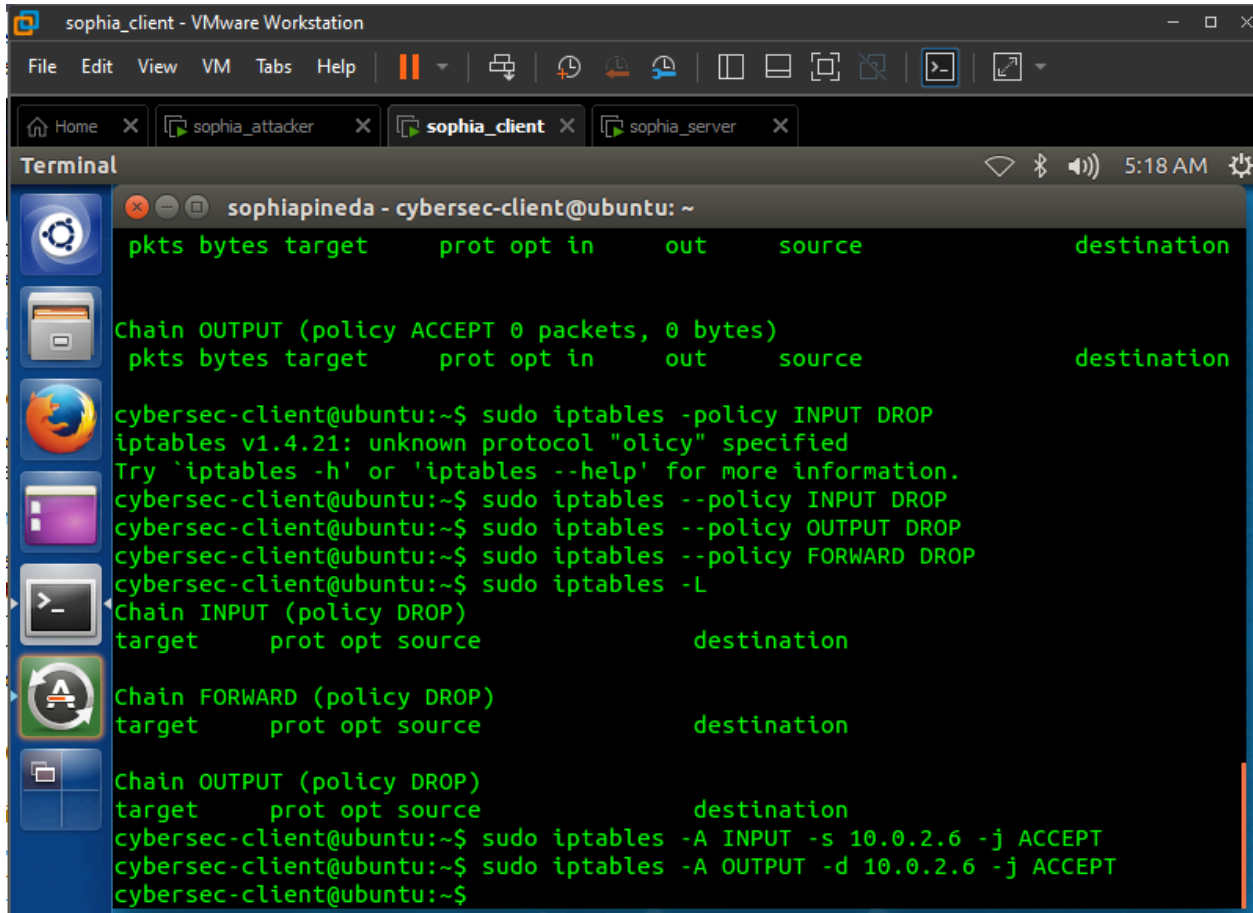
8. Enter `sudo iptables -L`
9. Enter `ping 10.0.2.8` in server VM



(adding rules to permit connection between server and client) **SCREENSHOT**

10. Enter `sudo iptables -A INPUT -s 10.0.2.6 -j ACCEPT` in client VM

11. Enter `sudo iptables -A INPUT -d 10.0.2.6 -j ACCEPT`



The screenshot shows a VMware Workstation window titled 'sophia_client - VMware Workstation'. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with icons for various VM actions, and a tab bar with three tabs: 'Home', 'sophia_attacker', and 'sophia_client' (which is active). Below the tabs is a 'Terminal' window. The terminal title bar reads 'sophiapineda - cybersec-client@ubuntu: ~'. The terminal content shows the following sequence of commands and output:

```
pkts bytes target      prot opt in      out      source      destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out      source      destination
cybersec-client@ubuntu:~$ sudo iptables -policy INPUT DROP
iptables v1.4.21: unknown protocol "olicy" specified
Try `iptables -h' or 'iptables --help' for more information.
cybersec-client@ubuntu:~$ sudo iptables --policy INPUT DROP
cybersec-client@ubuntu:~$ sudo iptables --policy OUTPUT DROP
cybersec-client@ubuntu:~$ sudo iptables --policy FORWARD DROP
cybersec-client@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target      prot opt source      destination
Chain FORWARD (policy DROP)
target      prot opt source      destination
Chain OUTPUT (policy DROP)
target      prot opt source      destination
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -s 10.0.2.6 -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -d 10.0.2.6 -j ACCEPT
cybersec-client@ubuntu:~$
```

12. Enter `sudo iptables -L` in client VM (checks rules) **SCREENSHOT**

```
sophia_client - VMware Workstation
File Edit View VM Tabs Help
Home X sophia_attacker X sophia_client X sophia_server X
Terminal File Edit View Search Terminal Help 5:19 AM
sophiapineda - cybersec-client@ubuntu: ~

Chain OUTPUT (policy DROP)
target      prot opt source                destination
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -s 10.0.2.6 -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -d 10.0.2.6 -j ACCEPT
cybersec-client@ubuntu:~$ sudp iptables -L
No command 'sudp' found, did you mean:
  Command 'sudo' from package 'sudo' (main)
  Command 'sudo' from package 'sudo-ldap' (universe)
  Command 'sup' from package 'sup' (universe)
  Command 'sfdp' from package 'graphviz' (main)
sudp: command not found
cybersec-client@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target      prot opt source                destination
ACCEPT     all  --  10.0.2.6                anywhere

Chain FORWARD (policy DROP)
target      prot opt source                destination

Chain OUTPUT (policy DROP)
target      prot opt source                destination
ACCEPT     all  --  anywhere                10.0.2.6
cybersec-client@ubuntu:~$
```

13. Enter `ssh cybersec-client@10.0.2.8` in attacker VM (creates SHH connection)

SCREENSHOT

```
sophia_attacker - VMware Workstation
File Edit View VM Tabs Help
Home X sophia_attacker X sophia_client X sophia_server X
Terminal File Edit View Search Terminal Help 5:21 AM
sophiapineda - cybersec-attacker@ubuntu: ~

cybersec-attacker@ubuntu:~$ ssh cybersec-client@10.0.2.8
^C
cybersec-attacker@ubuntu:~$
```

(adding rules to permit SHH connection) **SCREENSHOT**

14. Enter `sudo iptables -A INPUT -p tcp -dport ssh -s 10.0.2.7 -j ACCEPT` in client VM

15. Enter `sudo iptables -A OUTPUT -p tcp -sport ssh -d 10.0.2.7 -j ACCEPT` in client VM

The screenshot shows a VMware Workstation window titled 'sophia_client - VMware Workstation'. The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with icons for file operations and VM management, and a tab bar with four tabs: 'Home', 'sophia_attacker', 'sophia_client' (selected), and 'sophia_server'. The main area is a terminal window titled 'Terminal' with a status bar showing network, Bluetooth, and audio icons, along with the time '5:23 AM' and a settings icon. The terminal prompt is 'sophianineda - cybersec-client@ubuntu: ~'. A search bar at the top of the terminal says 'Search your computer and online sources'. The terminal output shows the following commands and results:

```
sophianineda - cybersec-client@ubuntu: ~  
Command 'sup' from package 'sup' (universe)  
Command 'sfdp' from package 'graphviz' (main)  
sudp: command not found  
cybersec-client@ubuntu:~$ sudo iptables -L  
Chain INPUT (policy DROP)  
target    prot opt source                destination  
ACCEPT    all  --  10.0.2.6                anywhere  
  
Chain FORWARD (policy DROP)  
target    prot opt source                destination  
  
Chain OUTPUT (policy DROP)  
target    prot opt source                destination  
ACCEPT    all  --  anywhere                10.0.2.6  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp -dport ssh -s 10.0.2.7 -j ACCEPT  
Bad argument `ssh'  
Try `iptables -h' or 'iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$
```

(remove rules) **SCREENSHOT**

16. Enter `sudo iptables -D OUTPUT -p tcp --sport ssh -d 10.0.2.7 -j ACCEPT` in client VM
17. Enter `sudo iptables -D INPUT -p tcp --dport ssh -s 10.0.2.7 -j ACCEPT` in client VM


```
sophiapineda - cybersec-client@ubuntu: ~  
Chain FORWARD (policy DROP)  
target      prot opt source                destination  
  
Chain OUTPUT (policy DROP)  
target      prot opt source                destination  
ACCEPT      all  --  anywhere             10.0.2.6  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp -dport ssh -s 10.0.2.7 -j ACCEPT  
Bad argument `ssh`  
Try `iptables -h' or 'iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp -sport ssh -d 10.0.2.7 -j ACCEPT  
Bad argument `ssh`  
Try `iptables -h' or 'iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp --sport ssh -d 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -D INPUT -p tcp --dport ssh -s 10.0.2.7 -j ACCEPT  
cybersec-client@ubuntu:~$
```

18. Reconfigure rules -

```
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7 -m state --state NEW,ESTABLISHED -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7 -m state --state NEW,ESTABLISHED -j ACCEPT
```

The screenshot shows a VMware Workstation interface with a terminal window open on the 'sophia_client' VM. The terminal output is as follows:

```
sophiapineda - cybersec-client@ubuntu: ~  
-j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7  
-j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp -sport ssh -d 10.0.2.7  
-j ACCEPT  
Bad argument `ssh'  
Try `iptables -h' or `iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp --sport ssh -d 10.0.2.7  
-j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -D INPUT -p tcp --dport ssh -s 10.0.2.7  
-j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7  
-m state --state NEW,ESTABLISHED -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7  
-m state --state NEW,ESTABLISHED -j ACCEPT  
Bad argument `state'  
Try `iptables -h' or `iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7  
-m state --state NEW,ESTABLISHED -j ACCEPT  
Bad argument `m'  
Try `iptables -h' or `iptables --help' for more information.  
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7  
-m state --state NEW,ESTABLISHED -j ACCEPT  
cybersec-client@ubuntu:~$
```

(verifies SSH connection between attacker and client) **SCREENSHOT**

19. Enter `sudo iptables -A INPUT -p tcp -dport ssh -s 10.0.2.7 -m state --state NEW,ESTABLISHED -j ACCEPT` in client VM
20. Enter `sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7 -m state --state NEW,ESTABLISHED -j ACCEPT` in client VM
21. Enter `ssh cybersec-client@10.0.2.8` in attacker VM **SCREENSHOT**



The screenshot shows a VMware Workstation interface with a terminal window titled 'sophiapineda - cybersec-client@ubuntu: ~'. The terminal displays the following commands and their outputs:

```
-j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp -s sport ssh -d 10.0.2.7
-j ACCEPT
Bad argument `ssh'
Try `iptables -h' or 'iptables --help' for more information.
cybersec-client@ubuntu:~$ sudo iptables -D OUTPUT -p tcp --sport ssh -d 10.0.2.7
-j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -D INPUT -p tcp --dport ssh -s 10.0.2.7
-j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
Bad argument `state'
Try `iptables -h' or 'iptables --help' for more information.
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
Bad argument `m'
Try `iptables -h' or 'iptables --help' for more information.
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ ssh cybersec-attacker@10.0.2.7
^C
cybersec-client@ubuntu:~$
```

22. Enter `sudo iptables -L -n` in client VM **SCREENSHOT**

```
sophia_client - VMware Workstation
File Edit View VM Tabs Help
sophia_attacker sophia_client sophia_server
Terminal File Edit View Search Terminal Help 5:32 AM
sophiapineda - cybersec-client@ubuntu: ~
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
Bad argument 'm'
Try 'iptables -h' or 'iptables --help' for more information.
cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7
-m state --state NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ ssh cybersec-attacker@10.0.2.7
^C
cybersec-client@ubuntu:~$ sudo iptables -L --line-numbers
Chain INPUT (policy DROP)
num target prot opt source destination
1 ACCEPT all -- 10.0.2.6 anywhere
2 ACCEPT tcp -- 10.0.2.7 anywhere tcp dpt:ssh s
tate NEW,ESTABLISHED

Chain FORWARD (policy DROP)
num target prot opt source destination

Chain OUTPUT (policy DROP)
num target prot opt source destination
1 ACCEPT all -- anywhere 10.0.2.6
2 ACCEPT tcp -- anywhere 10.0.2.7 tcp spt:ssh s
tate NEW,ESTABLISHED
cybersec-client@ubuntu:~$
```

SCREENSHOT

23. Enter `sudo iptables -D INPUT 2`
24. Enter `sudo iptables -L --line-numbers`

The screenshot shows a VMware Workstation window titled "sophia_client - VMware Workstation". The interface includes a menu bar (File, Edit, View, VM, Tabs, Help), a toolbar with icons for file operations and VM management, and a tab bar with four tabs: "Home", "sophia_attacker", "sophia_client" (active), and "sophia_server". The main area is a terminal window titled "Terminal" with a status bar showing "5:33 AM". The terminal prompt is "sophiapineda - cybersec-client@ubuntu: ~". The terminal output displays the configuration of iptables chains: FORWARD, OUTPUT, and INPUT, all with a policy of DROP. The FORWARD and OUTPUT chains are currently empty. The INPUT chain has one rule (line 1) that accepts all traffic from 10.0.2.6. The terminal also shows the commands used to configure the iptables: "sudo iptables -D INPUT 2" and "sudo iptables -L --line-numbers".

```
sophiapineda - cybersec-client@ubuntu: ~  
Chain FORWARD (policy DROP)  
num target      prot opt source                destination  
Chain OUTPUT (policy DROP)  
num target      prot opt source                destination  
1  ACCEPT        all  --  anywhere              10.0.2.6  
2  ACCEPT        tcp  --  anywhere              10.0.2.7             tcp spt:ssh s  
tate NEW,ESTABLISHED  
cybersec-client@ubuntu:~$ sudo iptables -D INPUT 2  
cybersec-client@ubuntu:~$ sudo iptables -L --line-numbers  
Chain INPUT (policy DROP)  
num target      prot opt source                destination  
1  ACCEPT        all  --  10.0.2.6              anywhere  
Chain FORWARD (policy DROP)  
num target      prot opt source                destination  
Chain OUTPUT (policy DROP)  
num target      prot opt source                destination  
1  ACCEPT        all  --  anywhere              10.0.2.6  
2  ACCEPT        tcp  --  anywhere              10.0.2.7             tcp spt:ssh s  
tate NEW,ESTABLISHED  
cybersec-client@ubuntu:~$
```

CHALLENGE
Screenshot Required:

sophia_client - VMware Workstation

File Edit View VM Tabs Help

Home X sophia_attacker X **sophia_client** X sophia_server X

Terminal 5:35 AM

sophianineda - cybersec-client@ubuntu: ~

Search your computer and online sources

```
num target prot opt source destination
1 ACCEPT all -- anywhere 10.0.2.6
2 ACCEPT tcp -- anywhere 10.0.2.7 tcp spt:ssh s
tate NEW,ESTABLISHED
cybersec-client@ubuntu:~$ sudo iptables -L -v
Chain INPUT (policy DROP 9 packets, 1572 bytes)
pkts bytes target prot opt in out source destination
988 83421 ACCEPT all -- any any 10.0.2.6 anywhere

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
960 80470 ACCEPT all -- any any anywhere 10.0.2.6
17 3539 ACCEPT tcp -- any any anywhere 10.0.2.7
tcp spt:ssh state NEW,ESTABLISHED
cybersec-client@ubuntu:~$
```

1. Commands used to configure Iptables on Cybersec-Server to permit HTTP, HTTPS and drop other traffic.

sophia_client - VMware Workstation

File Edit View VM Tabs Help

Home X sophia_attacker X **sophia_client** X sophia_server X

Terminal 5:37 AM

```
sophiapineda - cybersec-client@ubuntu: ~  
pkts bytes target    prot opt in     out    source destination  
988 83421 ACCEPT    all  --  any    any    10.0.2.6  anywhere  
  
Chain FORWARD (policy DROP 0 packets, 0 bytes)  
pkts bytes target    prot opt in     out    source destination  
  
Chain OUTPUT (policy DROP 0 packets, 0 bytes)  
pkts bytes target    prot opt in     out    source destination  
960 80470 ACCEPT    all  --  any    any    anywhere  10.0.2.6  
17  3539 ACCEPT    tcp  --  any    any    anywhere  10.0.2.7  
tcp snt:ssh state NEW,ESTABLISHED  
cybersec-client@ubuntu:~$ sudo iptables -P INPUT DROP  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -m state --state ESTABLISHED -j  
ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -m state --st  
ate NEW,ESTABLISHED -j ACCEPT  
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 443 -m state --s  
tate NEW,ESTABLISHED -j ACCEPT  
cybersec-client@ubuntu:~$
```

2. Iptables chain after adding the rules. (sudo iptables -L)

sophia_client - VMware Workstation

File Edit View VM Tabs Help

Home X sophia_attacker X **sophia_client** X sophia_server X

Terminal 5:37 AM

sophianineda - cybersec-client@ubuntu: ~

Search your computer and online sources

```
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT    all  --  10.0.2.6                anywhere
ACCEPT    all  --  anywhere                anywhere           state ESTABLISHED
ACCEPT    tcp  --  anywhere                anywhere           tcp dpt:http state
NEW,ESTABLISHED
ACCEPT    tcp  --  anywhere                anywhere           tcp dpt:https state
NEW,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT    all  --  anywhere                10.0.2.6
ACCEPT    tcp  --  anywhere                10.0.2.7           tcp spt:ssh state
NEW,ESTABLISHED
cybersec-client@ubuntu:~$
```