Cybersecurity Portfolio Project Report

Project Title: Configure IP ACLs to Mitigate Attacks
Tool Used: Cisco Packet Tracer
Student Name: Thabiso K Dzveta

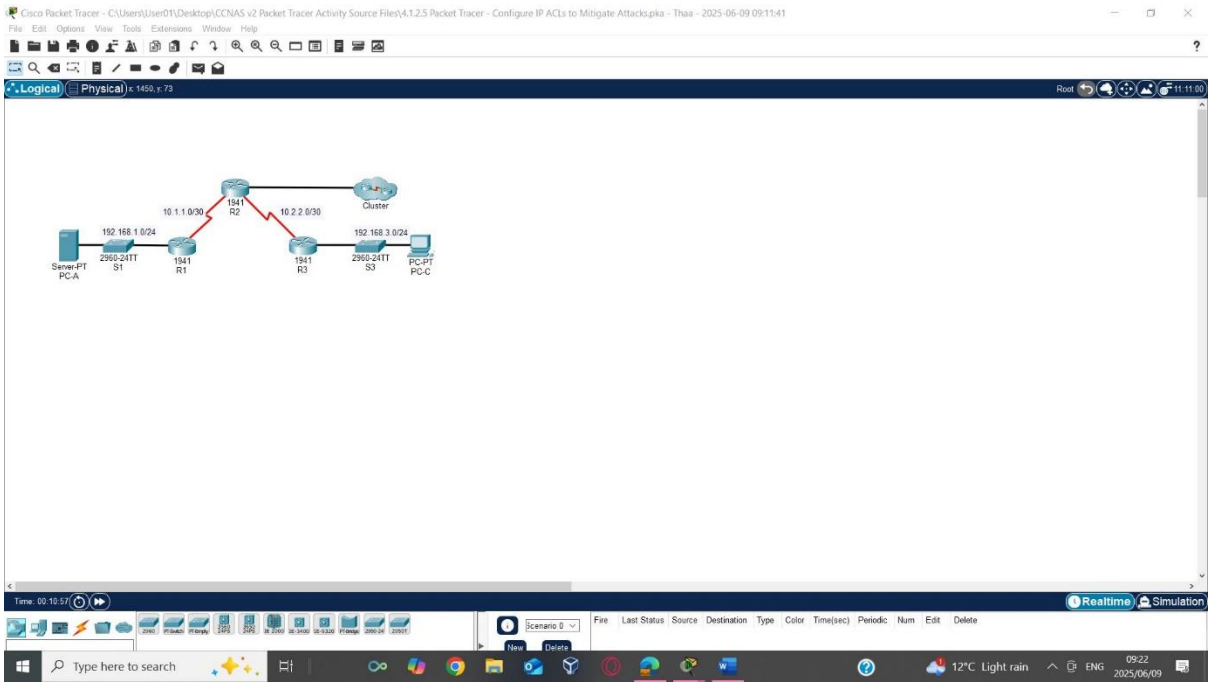
---

1. Project Overview

This project demonstrates how to secure a network by configuring IP Access Control Lists (ACLs) on Cisco routers. The objective was to restrict remote access to routers, filter traffic based on services, and prevent IP spoofing using ACLs.

---

2. Network Topology



3. IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252		N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252		
	G0/0	209.165.200.225	255.255.255.224		
	Lo0	192.168.2.1	255.255.255.0		
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252		N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

---

4. ACL Configuration Summary

ACL 10 - Remote Access Restriction

- **Purpose:** Allow only PC-C (192.168.3.3) to access routers via SSH.
- **Applied On:** VTY lines of R1, R2, R3
- **Commands:**

```
access-list 10 permit 192.168.3.3
access-list 10 deny any
line vty 0 4
 access-class 10 in
 login local
 transport input ssh
```

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
R1 con0 is now available




Press RETURN to get started.


User Access Verification

Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit 192.168.3.3
R1(config)#line vty 04
R1(config-line)#access-class 10 in
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1#
```

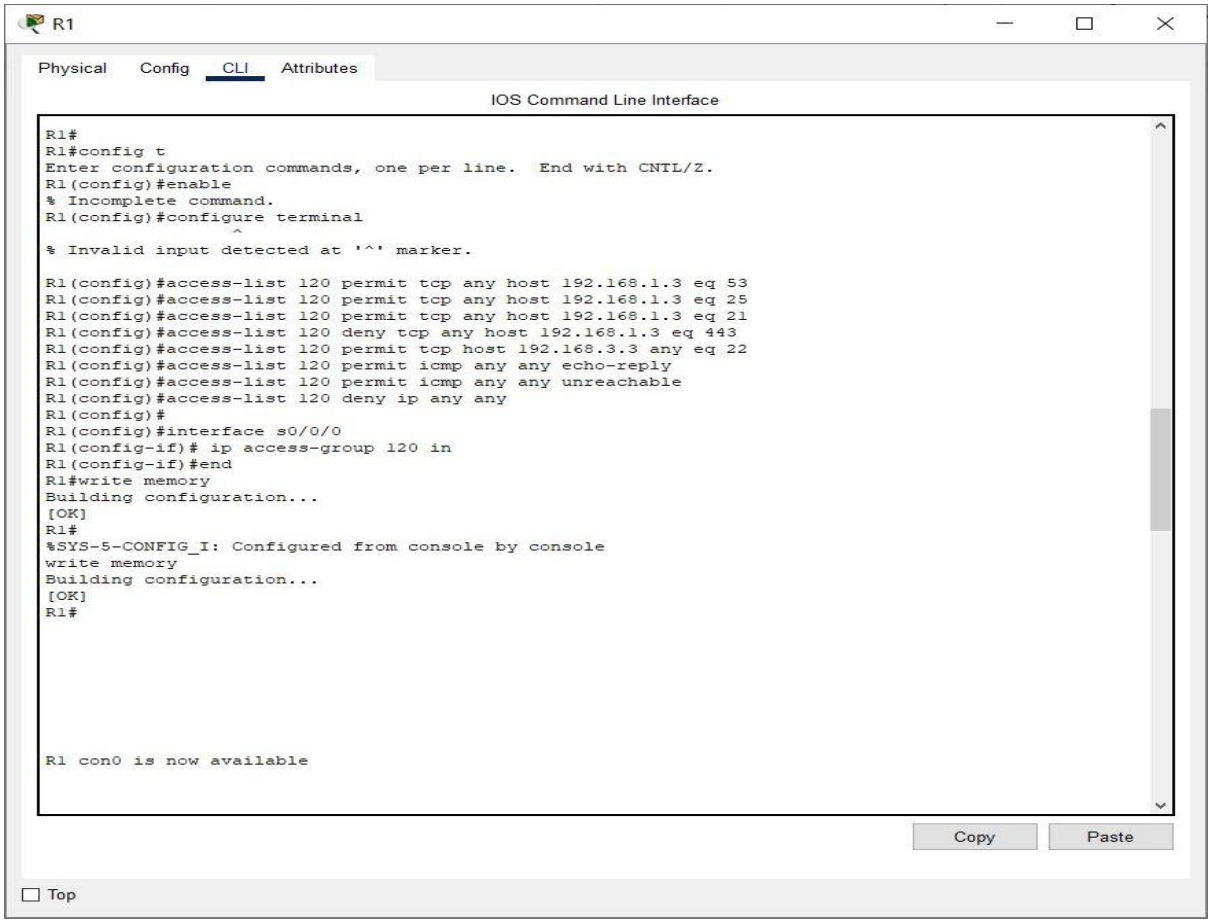
Copy Paste

Top

ACL 120 - Service Access Control (R1)

- **Purpose:**
  - Allow outside access to DNS, SMTP, and FTP on PC-A
  - Deny HTTPS access to PC-A
  - Permit SSH access from PC-C
  - Permit selected ICMP traffic
- **Applied On:** Interface S0/0/0 of R1 (inbound)
- **Commands:**

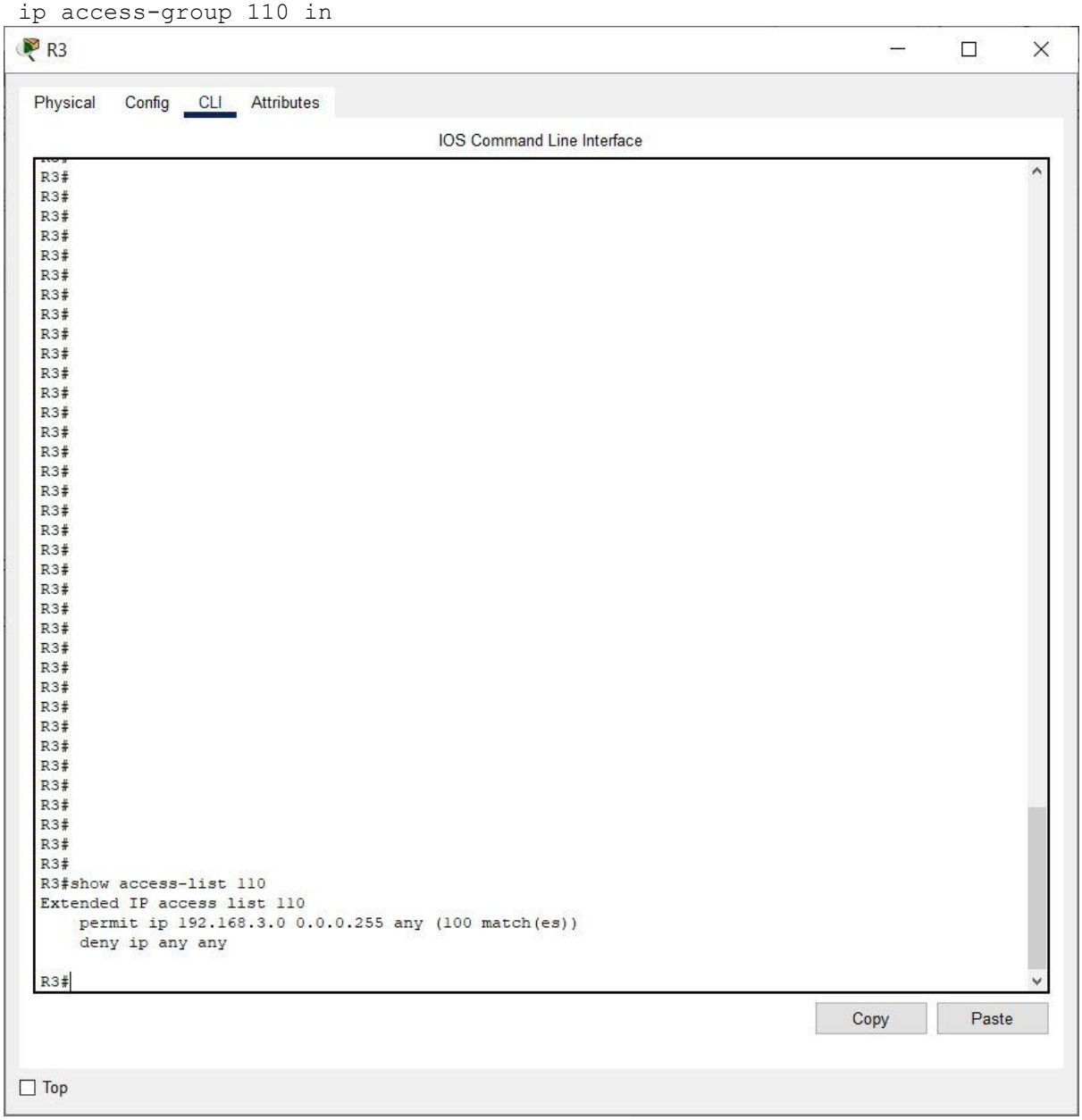
```
access-list 120 permit tcp any host 192.168.1.3 eq 53
access-list 120 permit tcp any host 192.168.1.3 eq 25
access-list 120 permit tcp any host 192.168.1.3 eq 21
access-list 120 deny tcp any host 192.168.1.3 eq 443
access-list 120 permit tcp host 192.168.3.3 any eq 22
access-list 120 permit icmp any any echo-reply
access-list 120 permit icmp any any unreachable
access-list 120 deny ip any any
interface s0/0/0
ip access-group 120 in
```



ACL 110 - Outbound Source IP Restriction (R3)

- **Purpose:** Deny any packet with a spoofed source IP that is not from the internal network.
- **Applied On:** Interface G0/1 of R3 (inbound)
- **Commands:**

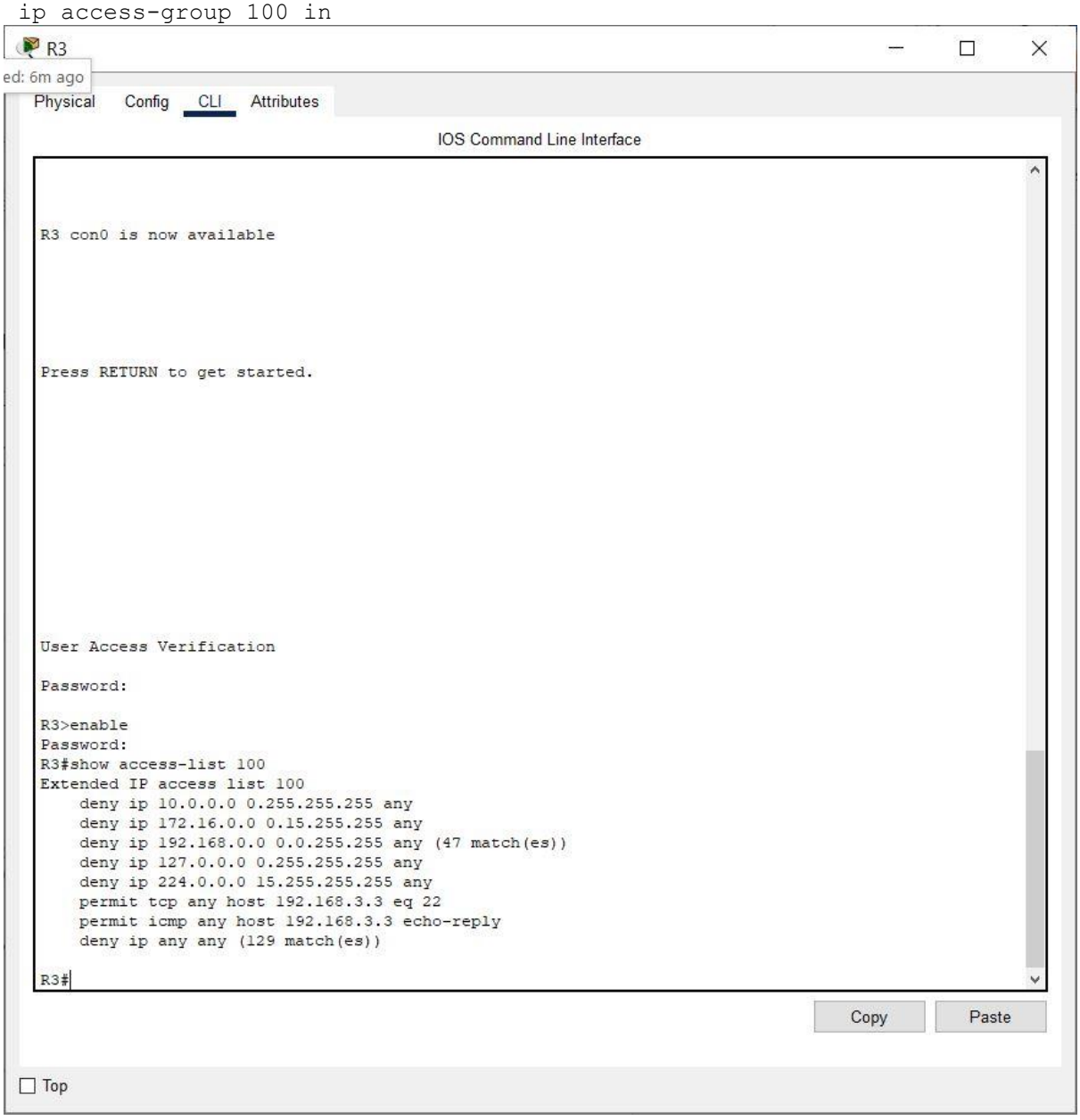
```
access-list 110 permit ip 192.168.3.0 0.0.0.255 any
access-list 110 deny ip any any
interface g0/1
 ip access-group 110 in
```



ACL 100 - Block Spoofed & Unauthorized Traffic (R3)

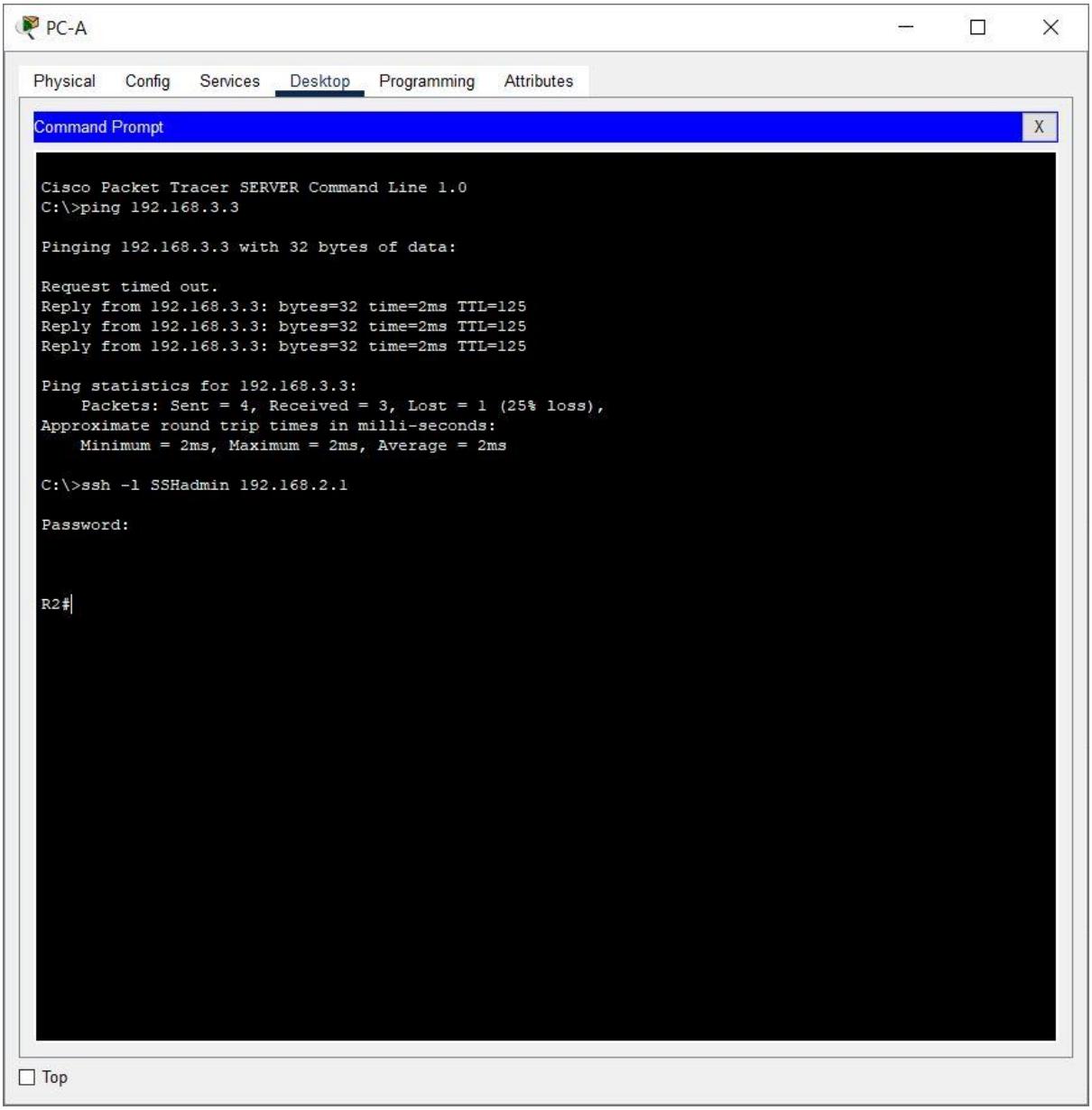
- **Purpose:** Block traffic from RFC 1918 private ranges, loopback, and multicast from the external interface.
- **Applied On:** Interface S0/0/1 of R3 (inbound)
- **Commands:**

```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 224.0.0.0 15.255.255.255 any
access-list 100 permit tcp any host 192.168.3.3 eq 22
access-list 100 deny ip any any
interface s0/0/1
 ip access-group 100 in
```

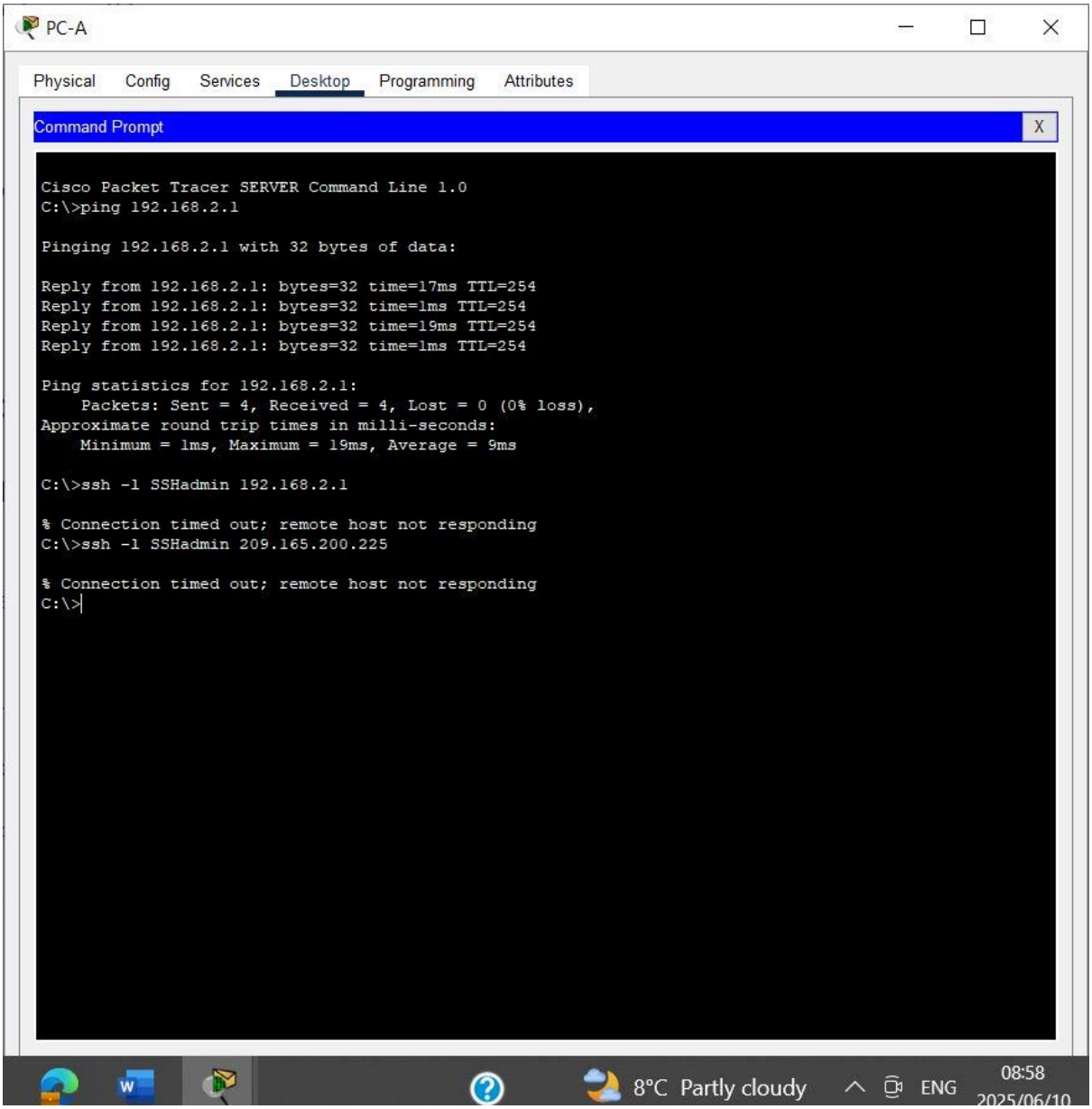


5. Verification Results

- Ping and SSH results from PC-A to R2 before and after ACLs
- **Before**



After



---

6. Conclusion

The successful implementation of multiple ACLs in this scenario demonstrates practical skills in securing network infrastructure using Cisco IOS. These configurations mitigate unauthorized access and spoofed IP attacks, a key component in cybersecurity defence strategies.

---

7. Reflection

This exercise enhanced my understanding of:

- The practical use of standard and extended ACLs
- Filtering traffic by IP, protocol, and port
- Applying ACLs to interfaces and VTY lines for security

[End of Report]