Q4

Securing SSH Access with Knockd

A. Installation and Configuration of Knockd [10 Marks]

1. Installing Knockd

To install Knockd on the VM, I used the following command:

```
sudo apt update && sudo apt install knockd -y
```

2. Configuring Knockd

The default configuration file is located at `/etc/knockd.conf`. I modified it as follows:

```
[options]
    UseSyslog

[openSSH]
    sequence = 4001, 5002, 6003
    seq_timeout = 10
    command = /usr/sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
    tcpflags = syn

[closeSSH]
    sequence = 6003, 5002, 4001
    seq_timeout = 10
    command = /usr/sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j
ACCEPT
    tcpflags = syn
```

3. Configuring iptables Rules

Before enabling Knockd, I set the default iptables rule to block SSH connections:

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

To ensure persistence across reboots, I used:

```
sudo apt install iptables-persistent
```

```
sudo netfilter-persistent save
```

4. Enabling and Starting Knockd

To enable and start the Knockd service:

```
sudo systemctl enable knockd
sudo systemctl start knockd
```

5. Testing the Configuration

To test the knocking sequence, I used:

```
knock -v <VM-IP> 4001 5002 6003  # Open SSH
ssh <user>@<VM-IP>
knock -v <VM-IP> 6003 5002 4001  # Close SSH
```

Choice of iptables Rules

- `-A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT` ensures that only the knocking client's IP is allowed.
- `-D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT` removes the rule to close SSH access.
- The `DROP` rule prevents unauthorized SSH attempts.
- Sequences were chosen to be non-trivial, avoiding common ones like `7000, 8000, 9000`.

B. Why Prefer TCP Over UDP? [2.5 Marks]

- **Reliability:** TCP ensures the knock packets reach the server reliably, whereas UDP packets might be lost due to network conditions.
- **Mitigation of Spoofing:** Since TCP involves handshaking, spoofing is harder compared to UDP, where packets can be easily forged.

C. Default Knockd Ports and Safety Concerns [2.5 Marks]

- **Default Ports:** The default knockd configuration uses the sequence `7000, 8000, 9000`.

- **Security Implications:**
  - These are commonly known ports, making them vulnerable to brute-force attacks.
  - Attackers scanning sequential ports might inadvertently trigger access.
  - Customizing the sequence reduces the likelihood of unauthorized access.

Conclusion

Knockd provides a lightweight method to secure SSH access by implementing port-knocking. Using TCP over UDP ensures reliable packet delivery and reduces spoofing risks. The default knock sequence is unsafe, and a custom sequence should be chosen to enhance security.