**Week 4: Firewalls, IDS, and IPS**

**Objective:** Set up and manage network defense mechanisms.

**Task#01:** **Configure a basic iptables firewall rule on a Linux VM to block a specific port.**

**Solution:**

**Explanation of the first command:**

* sudo: Executes the command with superuser privileges (necessary for iptables).
* iptables: The command-line utility for managing netfilter (the Linux kernel firewall).
* -A INPUT: Appends (adds to the end) the rule to the INPUT chain. The INPUT chain processes packets destined for the local machine.
* -p tcp: Specifies the protocol as TCP. You could use -p udp for UDP, or -p all for both.
* --dport 8080: Specifies the destination port as 8080.
* -j DROP: Specifies the target for matching packets. DROP means the packet is silently discarded, and no error message is sent back to the sender. An alternative is -j REJECT, which discards the packet but sends an error message (e.g., "Connection refused") back to the sender. DROP is generally preferred for security as it provides less information to potential attackers.

**Explanation of the second command:**

* -L: Lists all rules in all chains.
* -n: Shows numerical output (IP addresses and port numbers) instead of trying to resolve hostnames and service names, which is faster.
* -v: Provides verbose output, including packet and byte counts for each rule.

