Network Security Basics

This guide highlights some of the most important network security concepts and shows how they’re used in real life with simple examples.

# 1. Firewalls

A firewall is a network security system that acts as a digital barrier between a trusted network (like your computer or a company's internal network) and an untrusted one (like the Internet). Its main job is to monitor and control all incoming and outgoing network traffic based on predetermined security rules. This helps prevent unauthorized access and protects your system from malicious data and attacks.

## Types of Firewalls

* **Packet Filter**: Inspects each data packet and allows or denies it based on source/destination IP and port. Fast but limited.
* **Stateful Inspection**: Keeps track of active connections, making decisions with more context.
* **Web Application Firewall (WAF):** Protects web applications from attacks like SQL injection, XSS, etc..
* **Unified Threat Management (UTM):** Combines firewall with intrusion prevention, antivirus, and filtering.

## Example (Linux UFW)

$ sudo ufw status  
Status: active  
22/tcp ALLOW  
80/tcp DENY

This means SSH is allowed but HTTP traffic is blocked

Takeaway: Firewalls prevent unauthorized access and reduce potential attack surfaces.

# 2. VPN (Virtual Private Network)

A VPN creates a secure, encrypted connection (a tunnel) over the internet. It protects privacy and security by routing traffic through a remote server, hiding your real IP address.

## How a VPN Works

* Encryption: Data is scrambled into unreadable code
* IP Masking: Websites see the VPN server's IP instead of yours.
* Secure Tunneling: Prevents ISPs or hackers from spying on your data.

## Key Benefits

* Privacy from ISPs.
* Security: Protects data on public Wi-Fi.
* Access geo-blocking restrictions.

## Example

$ curl ifconfig.me  
Before VPN: 203.0.113.25  
After VPN: 10.8.0.2

Takeaway: Protects sensitive data on public networks.

# 3. HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is the secure version of HTTP. It uses SSL/TLS encryption to protect the communication between your browser and a website, ensuring data confidentiality and integrity.

## Key Features

* **Encryption**: Data (like passwords, credit cards) is secure.
* **Authentication**: Verifies the website is genuine.
* **Trust**: Modern browsers show a padlock icon when HTTPS is active.

## Example

$ curl -I https://example.com  
HTTP/2 200  
Strict-Transport-Security: max-age=31536000

Takeaway: Prevents attackers from intercepting or altering data.

# 4. Port Scanning

Port scanning is a technique used to identify open ports and services on a network. While attackers may use it to find vulnerabilities, administrators use it for auditing and securing networks.

## Types of Port Scans

* TCP Scan: connects fully
* UDP Scan: checks services like DNS, SNMP.
* SYN Scan: Half-open, harder to detect.

## Common Tool

- Nmap (Network Mapper)

## Examples

Ping Test:  
$ ping google.com  
64 bytes from 142.250.64.78: icmp\_seq=1 ttl=116 time=14.2 ms

Nmap Scan:  
$ nmap -p 22,80,443 192.168.1.1  
22/tcp open ssh  
80/tcp open http  
443/tcp closed https

## Best Practices / Ethics

Only scan systems you own or have permission for.  
 Disable unused ports and disable unnecessary services.