States of ports

TCP and UDP ports are in one of these three states depending on your needs:Open — The port responds to connection requests.Closed — The port is unreachable, indicating no corresponding service running.Filtered — The firewall monitors traffic and blocks specific port connection requests.

Security risks linked to open ports

Threat actors use open ports to carry out attacks and exploit vulnerabilities. Below, we share some common exploits and attacks that malicious actors leverage, and then detail two famous attacks via open port vulnerabilities.

Common exploits and attacksAn
open RDP connection
can be used to launch a credential-stuffing attack to access a server or deliver a ransomware payload.A
Denial of service (DoS) attack
sends many connection requests from various machines to disrupt a particular service. A typical example would be targeting the web ports of a web server to consume its bandwidth and resources, preventing legitimate users from accessing the service.Web service ports
are commonly used as entry points to launch attacks such as SQL injection and cross-site request forgery to exploit vulnerabilities within the applications themselves.Man-in-the-middle attacks
can be used to tap into unencrypted data traffic of well-

known ports to collect sensitive information. An example is the re-routing of data traffic to intercept email traffic.