Network Port Scan Report

Target IP Range: 172.20.10.0/24
Scan Date: 2025-05-25
Scanner Used: Nmap v7.94
Scan Type: TCP SYN Scan (-sS)
Scan Command:

```
nmap -sS 172.20.10.0/24 -oN network-scan.txt
```

Port	Protocol	State	Service	Notes
22	TCP	Open	SSH	Remote shell; secured, but check for brute force
80	TCP	Open	HTTP	Running lightweight web server (Apache)
139	TCP	Open	NetBIOS Session	Windows File Sharing - legacy, risky
445	TCP	Open	SMB	Check for SMB vulnerabilities (e.g., EternalBlue)
8000	TCP	Open	HTTP-alt	Custom admin panel (needs authentication check)

- **SMB (Port 445): High risk if exposed to the internet. Ensure patches are up-to-date and firewall rules are applied.**
- **HTTP on Port 80 and 8000: Web services should be checked for default credentials, directory listing, and known CVEs.**
- **NetBIOS (Port 139): Not needed unless using legacy file sharing. Recommend disabling if unused.**
- **SSH (Port 22): Ensure key-based authentication and strong passwords.**