■ TLS Clock Skew Lab

■ TLS Clock Skew Lab

■ Goal:
Break HTTPS by simulating a bad system clock.

■ Lab Setup:
- Ubuntu or Windows machine
- Change clock manually (e.g., set to 2020)
- Visit https://example.com or any HTTPS site

■ Result:
- Browser shows cert error: NET::ERR_CERT_DATE_INVALID
- TLS handshake fails due to expired/not-yet-valid cert

■ Fix Steps:
- Reset system time to current UTC
- Ensure NTP sync is working

■ Teaching Points:
- HTTPS depends on trust and time
- How does this affect malware, AV, and browsers?
- Could this break updates or cause false alerts?