Lab Report — Sniffing Network Traffic

Lab Report Template — Sniffing Network Traffic

Student: [Your Name] **Date:** [YYYY-MM-DD]

Capture Summary - Interface used: eth0 - Commands run: - sudo tcpdump -i eth0 -c 100 - sudo tcpdump -i eth0 -c 100 -nn - sudo tcpdump -i eth0 -c 100 icmp - sudo tcpdump -i eth0 port 80 -w juiceshop-web.pcap - sudo tcpdump -i eth0 -w PC-ftp.pcap

Findings - ICMP echo request/reply observed during ping test. - Plaintext HTTP POST to `/rest/user/login` observed (credentials redacted in public artifacts). - FTP file transfer observed between PC and Kali (pcap saved as PC-ftp.pcap).

Evidence (redacted) See `screenshots/` for redacted screenshots. Raw `.pcap` files are stored in private evidence repository.

Recommendations 1. Disable plaintext FTP; use SFTP/FTPS. 2. Enforce HTTPS and HSTS; never transmit credentials over HTTP. 3. Implement network monitoring and segment critical services.