# Lab 9 Rubric – DHCP Security

**Instructor:** Dr. Maryam R. Aliabadi

**Total Points:** 100

| Criteria | Excellent | Good | Satisfactory | Needs Improvement |
|---|---|---|---|---|
| **A. DHCP Server Configuration (20 points)** | DHCP server installed correctly; subnet, range, and gateway defined; service starts with no errors; client receives IP; clear screenshots of config + lease. | Mostly correct setup; minor syntax issues or one missing screenshot; IP assignment shown. | Partial configuration; client gets IP but configurations unclear or incomplete. | Incorrect or missing DHCP setup; no successful lease shown. |
| **B. Baseline Traffic Capture & DHCP Message Analysis (20 points)** | Correct tcpdump capture; clearly identifies DISCOVER/OFFER/REQUEST/ACK; screenshots readable; explanation accurate. | Capture mostly correct; minor errors in message identification or missing screenshot. | Attempted capture; limited or unclear analysis of messages. | No valid capture; messages not identified. |
| **C. DHCP Security Hardening (MAC filtering, interface binding, logging) (20 points)** | All security settings correctly implemented (deny MAC, interface binding, logging); tests show expected behavior; explanation of purpose of each control. | Mostly correct; one configuration incomplete or missing explanation. | Basic attempt; limited security settings; unclear results. | Incorrect or missing security configurations. |
| **D. Attack Simulations (15 points)** | Rogue DHCP shown (dnsmasq), MAC-filter denial seen in logs, starvation script executed correctly; captures show before/during/after traffic; analysis explains impact clearly. | Attacks mostly correct; minor issues in screenshots or explanations. | Partial attack execution; results unclear or not fully captured. | Attacks missing or incorrect; no evidence or analysis. |
| **E. Automation Script (dhcp_monitor.sh) & Cron Job (15 points)** | Script fully functional; detects anomalies (rogue offers, repeated DISCOVERs, exhaustion); clean output; cron job scheduled correctly; evidence included. | Script mostly functional; minor logic or output issues; cron job included. | Script present but minimally functional; limited evidence; cron job unclear. | Missing or nonfunctional script; no cron scheduling. |
| **F. Presentation & clear reporting (5 points)** | Report well-organized; correct filename; includes all screenshots, captures, and scripts; DOCX/PDF format as required. | Minor naming/formatting issues; small number of missing/unclear screenshots. | Formatting inconsistent; several missing items or unclear attachments. | Wrong filename/format; major missing deliverables. |