ARPGuard Facilitator Notes

Instructor/TA guide for delivery, troubleshooting, and grading cues

1. Session Goals

This session helps learners (a) connect ARP protocol mechanics to on-the-wire evidence, (b) recognize spoofing symptoms in captures, and (c) interpret explainable ARPGuard alerts without treating the tool as a black box. The lab is designed for deterministic grading using the provided PCAPs.

2. Recommended Timing (50–75 minutes)

- 5–10 min: ARP recap (broadcast who-has vs. is-at; ARP cache update behavior).
- 15–20 min: Phase 1 (benign PCAP) guided observation and field recording.
- 15–20 min: Phase 2 (attack PCAP) mapping conflict identification and MITM discussion.
- 10–15 min: Phase 3 run ARPGuard + interpret alerts (benign vs. attack).
- 5–10 min: Wrap-up + mitigations + assign reflection/quiz.

3. Pre-Lab Preparation Checklist

- Confirm all learners can open PCAPs in Wireshark and apply protocol display filters.
- Confirm Python environment is available if learners will run ARPGuard locally.
- Confirm repository structure is intact: code/, pcaps/, docs_pdf/, figures/.
- If time is limited, the lab can be completed using Wireshark observation only; ARPGuard can be demonstrated by the instructor.

4. Expected Outputs (Deterministic)

- **Benign capture:** stable mapping, no IP-to-MAC conflict; ARPGuard may emit 0 anomaly events (this is correct).
- **Attack capture:** at least one conflict where a protected IP maps to different MACs; ARPGuard should emit at least one anomaly event (typically IP_MAC_CONFLICT).
- The JSON outputs include a summary and PCAP metadata (hash/counts) to support TA validation.

5. Common Misconceptions (and Corrective Framing)

- **“ARP is the same as DNS.”** ARP resolves IPv4-to-MAC locally; DNS resolves names-to-IP at higher layers.
- **“Any ARP packet is malicious.”** ARP is normal; the signal is inconsistency (mapping conflicts, rapid flips).
- **“ARP spoofing only affects one host.”** Poisoning can target multiple victims or the gateway, enabling broader interception.
- **“If the attacker spoofs the gateway, traffic must break.”** A MITM attacker can forward traffic to remain stealthy; dropping yields obvious DoS.

6. Troubleshooting

If learners see no ARP packets in Wireshark:

- Confirm the display filter is: **arp** (not a capture filter).
- Confirm the correct PCAP file is opened.

If ARPGuard fails to run:

- Install dependencies: **pip install -r requirements.txt**
- Confirm scapy can import (if used): **python -c "from scapy.all import rdpcap; print('ok')"**
- Ensure commands are executed from the repository root so relative paths resolve.

7. Grading Guidance

The quiz answer key includes correct answers and short justifications. If a learner’s response is directionally correct but lacks justification, partial credit can be assigned; however, the teaching goal is that learners can explain *why*, not only *what*. The lab reflection can be graded using the rubric in the lab handout (evidence quality + correctness + interpretation).

8. Extensions (Optional)

- Discuss enterprise mitigations: DHCP snooping + Dynamic ARP Inspection, 802.1X, VLAN segmentation and blast-radius reduction.
- Have learners propose a context-aware rule that reduces false positives (e.g., whitelist gateway MAC, allow failover windows).
- Compare ARP spoofing with IPv6 Neighbor Discovery threats and mitigation differences.

References

[1] D. C. Plummer, “An Ethernet Address Resolution Protocol,” RFC 826, IETF, Nov. 1982.

[2] S. Cheshire, “IPv4 Address Conflict Detection,” RFC 5227, IETF, July 2008.

[4] Cisco Systems, “Dynamic ARP Inspection (DAI),” security configuration documentation.

[5] IEEE, “IEEE 802.1X Port-Based Network Access Control,” standard overview.