ARPGuard Facilitator Notes

ARPGuard — Facilitator Notes (Instructor / TA)
==========
1. Recommended Timing (50–75 minutes)

- 5–10 min: ARP recap (broadcast request vs. unicast reply; ARP cache concept)
- 15–20 min: Phase 1 (benign PCAP) guided observation
- 15–20 min: Phase 2 (attack PCAP) guided observation and discussion
- 10–15 min: Phase 3 ARPGuard run + alert interpretation
- 5–10 min: Wrap-up + mitigations + reflection prompt
2. Setup Checklist

- Ensure learners can open PCAPs in Wireshark.
- Ensure Python 3.11+ is available if learners will run ARPGuard locally.
- If time is limited, the lab can be completed purely via Wireshark observation and discussion using the PCAPs.
3. Common Misconceptions and How to Address Them

A) “ARP is the same as DNS.”
- Correction: ARP resolves IPv4→MAC on a local segment; DNS resolves names→IP at higher layers.
B) “Any ARP packet is malicious.”
- Correction: ARP is normal for local address resolution. The signal is inconsistency (e.g., IP→MAC changes).
C) “ARP spoofing only affects one machine.”
- Correction: Poisoning can target multiple hosts (victims) and/or the gateway, enabling broader interception.
D) “If the attacker spoofs the gateway, traffic always breaks.”
- Correction: A MITM attacker can forward traffic to remain stealthy; drops yield obvious DoS.
4. Troubleshooting Notes

- If learners see no ARP packets, confirm Wireshark display filter uses: arp
- If ARPGuard fails to run:
- Verify dependencies installed: pip install -r requirements.txt
- Verify scapy import works: python -c "from scapy.all import rdpcap; print('ok')"
5. Teaching Emphasis (Why the Alerts Make Sense)

ARPGuard uses explainable heuristics, so the facilitator can tie alerts back to observable evidence:
- IP_MAC_CONFLICT: the same IP address is associated with multiple MAC addresses over time.
This should be visible directly in Wireshark by comparing the sender hardware addresses in ARP replies.
- UNSOLICITED_REPLY: ARP replies that are not clearly triggered by a recent who-has request.
Emphasize that this can be benign (gratuitous ARP), so ARPGuard treats it as a softer indicator.
6. Discussion Prompts (Mitigations and Defense-in-Depth)

- What changes if the network enforces DHCP snooping + Dynamic ARP Inspection (DAI)?
- Why do static ARP entries reduce spoofing risk, and what operational cost do they introduce?
- How does segmentation (VLANs) reduce the blast radius of ARP poisoning?
- What monitoring signals might complement ARPGuard (switch logs, IDS, host ARP cache audits)?
7. Answer Key Alignment

The quiz answer key includes both the correct answer and a short justification.
If a learner’s answer is directionally correct but lacks justification, partial credit can be assigned, but the rubric
goal is that learners can explain “why,” not only “what.”
8. References
---
[1] D. C. Plummer, “An Ethernet Address Resolution Protocol,” RFC 826, Nov. 1982.